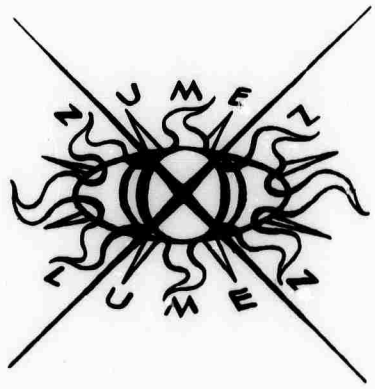
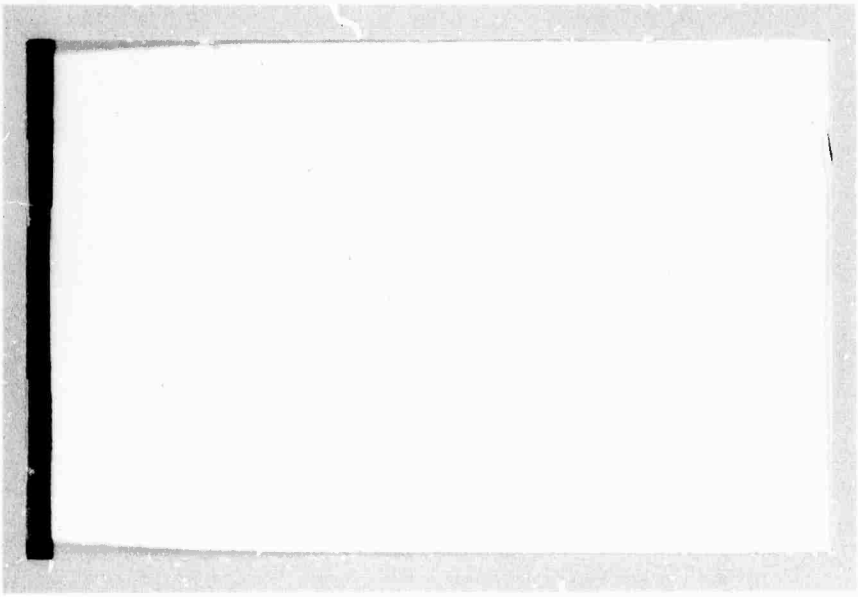
THE UNIVERSITY OF WISCONSIN





MATHEMATICS RESEARCH CENTER

Address:

Mathematics Research
Center
The University of Wisconsin
Madison, Wisconsin 53706
U.S.A.

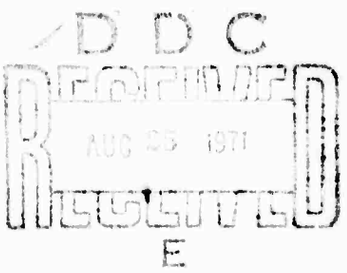
THE UNIVERSITY OF WISCONSIN
MATHEMATICS RESEARCH CENTER

Contract No. : DA-31-124-ARO-D-462

SOME TECHNIQUES FOR CONSTRUCTING MUTUALLY ORTHOGONAL LATIN SQUARES

W. T. Federer, A. Hedayat, E. T. Parker
B. L. Raktoe, Esther Seiden, and R. J. Turyn

MRC Technical Summary Report #1030
June 1971



Received December 17, 1969

Madison, Wisconsin 53706

AR 70-31 Unclassified

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)
Mathematics Research Center
University of Wisconsin, Madison, Wis. 53706

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP
None

3. REPORT TITLE
SOME TECHNIQUES FOR CONSTRUCTING MUTUALLY ORTHOGONAL LATIN SQUARES

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)
Summary Report: no specific reporting period.

5. AUTHOR(S) (First name, middle initial, last name)
W. T. Federer, A. Hedayat, E. T. Parker, B. L. Raktoe, Esther Seiden, and R. J. Turyn

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
June 1971	119	56

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
Contract No. DA-31-124-ARO-D-462	#1030
b. PROJECT NO. None	
c.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
d.	None

10. DISTRIBUTION STATEMENT
Distribution of this document is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
None	Army Research Office-Durham, N.C.

13. ABSTRACT

The methods of confounding, fractional replication, analysis of variance, group, projecting diagonals, orthomorphism, oval, code, pairwise balanced design, product composition, sum composition and computer construction of a set of mutually orthogonal latin squares are discussed.

DD FORM 1 NOV 65 1473

Unclassified

Security Classification

AGO 5698A

TABLE OF CONTENTS

ABSTRACT

Various methods of constructing a set of mutually orthogonal latin squares are presented and the theoretical aspects of various methods are discussed. Illustrative examples of constructing latin squares and sets of mutually orthogonal latin squares are given. The methods of constructing latin squares and sets of orthogonal latin squares are complete and partial confounding, fractional replication, analysis of variance, group, projecting diagonals, orthomorphism, pairwise balanced design, oval, code, product composition, and sum composition. The methods of construction designated as partial confounding, fractional replication, analysis of variance, and sum composition appear not to have been discussed previously in the literature. The methods of complete confounding and of projecting diagonals have been discussed; the actual construction procedure has been illustrated with several examples. The sum composition method has interesting consequences in combinatorial theory as well as in the construction of orthogonal latin squares. Lastly, equivalences of fourteen combinatorial systems to orthogonality in latin squares has been investigated and described.

BLANK PAGE

SOME TECHNIQUES FOR CONSTRUCTING MUTUALLY ORTHOGONAL LATIN SQUARES

W. T. Federer[1], A. Hedayat[2], E. T. Parker[3]
B. L. Raktoe[4], Esther Seiden[5], and R. J. Turyn[6]

I. Introduction and Some Terminology

The purpose of this paper is to present a set of methods for constructing mutually orthogonal latin squares and to exhibit some squares produced by each of the methods. The set of methods presented herein was discussed in a series of informal seminars held during the weeks of July 14-18 and 21-25, 1969, by the authors at Cornell University. The motivation for these discussion was derived from results obtained by Hedayat [1969] and from the optimism of the authors. New procedures for constructing a set of mutually orthogonal latin squares and new views of present methods of construction were desired in order to advance the theory of mutual orthogonality in latin squares.

---

[1] Professor of Biological Statistics, Cornell University and Visiting Professor, Mathematics Research Center, University of Wisconsin (on sabbatical leave 1969-70).

[2] Assistant Professor, Cornell University.

[3] Professor of Mathematics, University of Illinois, and Visiting Professor, Cornell University (July, 1969).

[4] Associate Professor, University of Guelph and Visiting Associate Professor, Cornell University (January to August, 1969).

[5] Professor, Michigan State University, and Visiting Professor, Cornell University (June, July, August, 1969).

[6] Mathematician, Raytheon Corporation, and Visiting Professor, Cornell University (July, 1969).

Sponsored by the United States Army under Contract No.: DA-31-124-ARO-D-462.

As may be noted from the table of contents, the different sections were written by different authors. An attempt was made to have a consistent notation and a uniform style. Although much more work is required to finalize the method in several of the sections enough is known about the method to use it to construct a latin square of any order or to construct a set of two or more mutually orthogonal latin squares. Also, a number of equivalences may be noted for some of the methods.

The theory of mutual orthogonality in latin squares has application in the construction of many classes of experiment designs and in many combinatorial systems. The latter subject is discussed in section XV where the equivalences of various combinatorial systems are presented. With regard to the former subject, there is an ever present need for new experiment designs for new experimental situations in order for the experimenter not to have to conduct his experiment to fit known experiment designs.

Some of the notation and terminology that will be utilized is presented below.

Definition I.1. A latin square of order n on a set $\sum$ with n distinct elements is an $n \times n$ matrix each of whose rows and columns is a permutation of the set $\sum$.

Example:

1	2	3
2	3	1
3	1	2

is a latin square of order 3 on $\sum = \{1,2,3\}$.

Definition I.2. Two latin squares $L_1 = (a_{ij})$ and $L_2 = (b_{ij})$ of order n are said to be orthogonal if the n^2 ordered pairs (a_{ij}, b_{ij}) $(i,j = 1,2,\ldots,n)$ are all distinct. Note that L_1 and L_2 need not be defined on the same set.

Example:

1	2	3
2	3	1
3	1	2

and

A	B	C
C	A	B
B	C	A

.

Definition I.3. The members of a set of t latin squares $L_1, L_2, \ldots, L_t$ of order n are said to be mutually (pairwise) orthogonal if L_i is orthogonal to L_j, $i \neq j$, $i,j = 1,2,\ldots,t$. Hereafter by an $O(n,t)$ set we mean a set consisting of t mutually orthogonal latin squares of order n.

Example:

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

,

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

, and

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

.

Latin squares and orthogonal latin squares have at least 187 years of history. Hedayat [1969], Section IX has presented a reasonably good picture of this history which will not be repeated here. It is planned to prepare a historical account of developments related to orthogonality in latin squares and to publish this material together with a bibliography elsewhere.

II. Factorial Confounding Construction of O(n,t) Sets

II.1. Complete Confounding

A factorial treatment design consists of all possible combinations of two or more factors each at two or more levels. The set of all combinations of m factors each at n levels is denoted as an n^m factorial; for n a prime power the main effects and interaction effects in an n^m factorial are in a 1:1 correspondence with the points of the finite projective geometry $PG(m-1,n)$. For example, the n^2 factorial consists of two main effects, say A and B with levels $(A)_i$ and $(B)_j$ respectively, $i,j = 0,1,2,\ldots,n-1$, and $n-1$ two factor interactions AB^{u_s}, $s = 1,2,\ldots,n-1$ with levels $(AB^{u_s})_{u_i+u_s u_j}$ for $u_i + u_s u_j = u_0, u_1, u_2, \ldots, u_{n-1}$ where the u_i are elements of the Galois field $GF(n)$, and the $n+1$ effects are in a 1:1 correspondence with the points of $PG(1,n)$. Each of the $n+1$ effects is associated with a set of $n-1$ single-degree-of-freedom-contrast parameters making a total of $(n+1)(n-1) = n^2-1$ parameters; if the mean is adjoined to the set of contrasts then the n^2 single-degree-of-freedom-contrast parameters are in a 1:1 correspondence with the points of the finite Euclidean geometry $EG(2,n)$. Therefore, the n^2 combinations $u_i u_j$ are in a 1:1 correspondence with the n^2 single-degree-of-freedom-contrast parameters in $EG(2,n)$.

For $n = 4$, the levels of the main effects and interactions are given by $(A)_i$, $(B)_j$, and $(AB^{u_s})_{u_i+u_s u_j}$, where $u_0 = 0, u_1 = 1, u_2 = x, u_3 = 1+x = x^2$ are the marks of $GF(4)$, $i,j = 0, 1, 2, 3$, and $s = 1, 2, 3$. Let $(A)_i$ be the rows and $(B)_j$ be the columns of a latin square of order 4 as follows:

	column 1 = $(B)_0$	column 2 = $(B)_1$	column 3 = $(B)_2$	column 4 = $(B)_3$
row 1 = $(A)_0$	00	01	02	03
row 2 = $(A)_1$	10	11	12	13
row 3 = $(A)_2$	20	21	22	23
row 4 = $(A)_3$	30	31	32	33

In the above only the subscript of the combination u_iu_j and of the effects A and B is given for each row-column intersection. Thus, $(A)_{u_0} = (A)_0$ consists of the $n=4$ subscripts $00,01,02,03$ of the combinations u_0u_0, u_0u_1, u_0u_2, u_0u_3. The remaining levels are similarly defined.

A symbol in a latin square corresponds to those combinations u_iu_j for which $u_i + u_su_j$ for interaction effect AB^{u_s}, is a constant, with each constant corresponding to one of the n symbols in the latin square of order n. Also, $n-1$ latin squares of order n may be formed for $s = 1, 2, \ldots,$ and $n-1$; this set of latin squares forms an $O(n, n-1)$ set. For $n = 4$ the $O(4,3)$ set is formed as follows (additional detail may be found in Mann [1949], chapter VIII, Kempthorne [1952], pages 331-340, and Federer [1955], chapters VII, IX and XV):

$$(AB^{u_1})_{u_i+u_1u_j} = \begin{cases} u_0\ 00 + 11 + 22 + 33 \rightarrow \text{I} \\ u_1\ 01 + 10 + 23 + 32 \rightarrow \text{II} \\ u_2\ 02 + 13 + 20 + 31 \rightarrow \text{III} \\ u_3\ 03 + 12 + 21 + 30 \rightarrow \text{IV} \end{cases}$$

00 = I	01 = II	02 = III	03 = IV
10 = II	11 = I	12 = IV	13 = III
20 = III	21 = IV	22 = I	23 = II
30 = IV	31 = III	32 = II	33 = I

$$(AB^{u_2})_{u_i+u_2u_j} = \begin{cases} u_0\ 00 + 13 + 21 + 32 \to \alpha \\ u_1\ 03 + 10 + 22 + 31 \to \beta \\ u_2\ 01 + 12 + 20 + 33 \to \gamma \\ u_3\ 02 + 11 + 23 + 30 \to \delta \end{cases}$$

α	γ	δ	β
β	δ	γ	α
γ	α	β	δ
δ	β	α	γ

$$(AB^{u_3})_{u_i+u_3u_j} = \begin{cases} u_0\ 00 + 12 + 23 + 31 \to W \\ u_1\ 02 + 10 + 21 + 33 \to X \\ u_2\ 03 + 11 + 20 + 32 \to Y \\ u_3\ 01 + 13 + 22 + 30 \to Z \end{cases}$$

W	Z	X	Y
X	Y	W	Z
Y	X	Z	W
Z	W	Y	X

where the first column to the right of the brace represents the u_i obtained from the subscript.

In the above the complete confounding scheme of sources of variation in the $O(4, 3)$ set and the effects in the factorial may be illustrated in the following analysis of variance table wherein the total sum of squares has been orthogonally decomposed into the sums of squares related to the above confounding scheme as follows:

Source of variation	Degrees of freedom
Correction for mean	1
Rows = A effect	3
Columns = B effect	3
Roman numbers = (AB^{u_1}) effect	3
Greek letters = (AB^{u_2}) effect	3
Latin letters = (AB^{u_3}) effect	3
Total	16

Instead of relating the mutually orthogonal latin squares of order 4 to a 4^2 factorial we may relate them to a 2^4 factorial in the following manner, i.e., we consider $EG(4, 2)$ and $GF(2)$ with elements 0 and 1. Let the 16 row-column intersections be numbered as follows:

	column			
row	1	2	3	4
1	0000	0001	0010	0011
2	0100	0101	0110	0111
3	1000	1001	1010	1011
4	1100	1101	1110	1111

where the subscripts in the above table represent the combination $a_g b_h c_i d_j$ of the factors a, b, c, and d with two levels (0 and 1) each.* The rows correspond to factorial effects A, B, and AB and the columns correspond to factorial effects C, D, and CD . (This form of constructing latin squares has been used by Fisher and Yates [1957] for latin squares of order 8 and by Federer [1955]). Then, let the symbols in the 3 latin squares be represented by the following scheme:

Factorial generators	Combinations	latin squares
$(AC)_0$, $(BD)_0$, $(ABCD)_0$	0000 + 0101 + 1010 + 1111 = I	I II III IV
$(AC)_0$, $(BD)_1$, $(ABCD)_1$	0001 + 0100 + 1011 + 1110 = II	II I IV III
$(AC)_1$, $(BD)_0$, $(ABCD)_1$	0010 + 0111 + 1000 + 1101 = III	III IV I II
$(AC)_1$, $(BD)_1$, $(ABCD)_0$	0011 + 0110 + 1001 + 1100 = IV	IV III II I
$(AD)_0$, $(ABC)_0$, $(BCD)_0$	0000 + 0110 + 1011 + 1101 = W	W Z X Y
$(AD)_0$, $(ABC)_1$, $(BCD)_1$	0010 + 0100 + 1001 + 1111 = X	X Y W Z
$(AD)_1$, $(ABC)_0$, $(BCD)_1$	0001 + 0111 + 1010 + 1100 = Z	Y X Z W
$(AD)_1$, $(ABC)_1$, $(BCD)_0$	0101 + 0011 + 1000 + 1110 = Y	Z W Y X
$(ACD)_0$, $(BC)_0$, $(ABD)_0$	0000 + 0111 + 1110 + 1001 = α	α γ δ β
$(ACD)_0$, $(BC)_1$, $(ABD)_1$	1010 + 0100 + 0011 + 1101 = β	β δ γ α
$(ACD)_1$, $(BC)_0$, $(ABD)_1$	1000 + 0110 + 1111 + 0001 = γ	γ α β δ
$(ACD)_1$, $(BC)_1$, $(ABD)_0$	0010 + 0101 + 1011 + 1100 = δ	δ β α γ

* Note: Some authors use lower case letters to denote the factors and capital letters to denote effects or levels of effects; we follow that usage here.

The correspondence of the latin squares obtained from complete confounding considering a 4^2 factorial and considering a 2^4 factorial is demonstrated in the following analysis of variance table:

Source of variation		degrees of freedom	
Correction for mean		1	
Rows	= A effect in r^2 factorial	3	
	A effect in 2^4 factorial		1
	B " " 2^4 "		1
	AB " " 2^4 "		1
Columns	= B effect in 4^2 factorial	3	
	C effect in 2^4 factorial		1
	D " " 2^4 "		1
	CD " " 2^4 "		1
Roman numbers	= AB^{u_1} effect in 4^2 factorial	3	
	AC effect in 2^4 factorial		1
	BD " " 2^4 "		1
	ABCD " " 2^4 "		1
Greek letters	= AB^{u_2} effect in 4^2 factorial	3	
	ACD effect in 2^4 factorial		1
	BC " " 2^4 "		1
	ABD " " 2^4 "		1
Latin letters	= AB^{u_3} effect in 4^2 factorial	3	
	AD effect in 2^4 factorial		1
	ABC " " 2^4 "		1
	BCD " " 2^4 "		1
Total		16	

It should be noted here that the effects in the 2^4 map directly into the 4^2 projective geometry or $PG(1,2^2)$. Likewise, even though <u>one</u> more set of generators is available, <u>viz</u>,

	Generators	interaction
Roman numbers	= AD, BC	ABCD
Greek letters	= AC, ABD	BCD
Latin letters	= BD, ABC	ACD

the three orthogonal latin squares produced are the same ones. Since the third effect above is obtained as the product of two generators (exponents mod 2) we need consider only two generators. Multiplying these by CD (exponents mod 2) we obtain the generators of the preceding scheme. Hence, even though two dif - ferent complete confounding schemes are available there is a simple one-to-one mapping of one set into the other set. Although nothing interesting turns up here, it would be interesting to study the various complete confounding schemes in the latin square of order 9 as related to the 3^4 factorial.

As a second illustration of the use of complete confounding to construct latin squares, let us consider a latin square of order 6 . Using the notation and concepts of Raktoe [1969] on mixed prime factorials as related to rings and elements of ideals in the rings we designate the 6^2 as a $2^2(3)^2$ factorial and represent a combination by ghij where g, h are members of the ideal I (3) and i, j are members of the ideal I (4) . The effects in the 2^2 and in the 3^2 factorials are denoted respectively by:

A^3	C^4
B^3	D^4
A^3B^3	C^4D^4
	C^4D^2

The remaining interactions are given below in the analysis of variance table:

Source of variation	Degrees of freedom	
Correction for mean	1	
Rows = A^3C^4	5	
A^3		1
C^4		2
$A^3 \times C^4$		2
Columns = B^3D^4	5	
B^3		1
D^4		2
$B^3 \times D^4$		2
Treatments or symbols = $A^3B^3C^4D^4$	5	
A^3B^3		1
C^4D^4		2
$A^3B^3 \times C^4D^4$		2
Remainder	20	
C^4D^2		2
$A^3 \times D^4$		2
$A^3 \times C^4D^4$		2
$A^3 \times C^4D^2$		2
$B^3 \times C^4$		2
$B^3 \times C^4D^4$		2
$B^3 \times C^4D^2$		2
$A^3B^3 \times C^4$		2
$A^3B^3 \times D^4$		2
$A^3B^3 \times C^4D^2$		2
Total	36	

Let us now set up the 6 rows and the 6 columns of a latin square of order 6 with the corresponding designation of the 36 combinations as follows:

Columns

Rows	$(B^3D^4)_0$	$(B^3D^4)_1$	$(B^3D^4)_2$	$(B^3D^4)_3$	$(B^3D^4)_4$	$(B^3D^4)_5$
$(A^3C^4)_0$	0000	0304	0002	0300	0004	0302
$(A^3C^4)_1$	3040	3344	3042	3340	3044	3342
$(A^3C^4)_2$	0020	0324	0022	0320	0024	0322
$(A^3C^4)_3$	3000	3304	3002	3300	3004	3302
$(A^3C^4)_4$	0040	0344	0042	0340	0044	0342
$(A^3C^4)_5$	3020	3324	3022	3320	3024	3322

Now let the levels of $A^3B^3C^4D^4$ correspond to the symbols in a latin square of order 6 as follows:

Levels	Combination for which $3g+3h+4i+4j$, mod 6, is constant		Symbol
$(A^3B^3C^4D^4)_0$	0000 + 3342 + 0024 + 3300 + 0042 + 3324	→	0
$(A^3B^3C^4D^4)_1$	0304 + 3040 + 0322 + 3004 + 0340 + 3022	→	1
$(A^3B^3C^4D^4)_2$	0002 + 3344 + 0020 + 3302 + 0044 + 3320	→	2
$(A^3B^3C^4D^4)_3$	0300 + 3042 + 0324 + 3000 + 0342 + 3024	→	3
$(A^3B^3C^4D^4)_4$	0004 + 3340 + 0022 + 3304 + 0040 + 3322	→	4
$(A^3B^3C^4D^4)_5$	0302 + 3044 + 0320 + 3002 + 0344 + 3020	→	5

This produces the following latin square of order 6:

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Alternatively we could have used levels of $A^3B^3C^4D^2$ to construct the following latin square of order 6:

Levels	Combinations for which $3g+3h+4i+2j$, mod 6, is constant	Symbol
$(A^3B^3C^4D^2)_0$	0000 + 3344 + 0022 + 3300 + 0044 + 3322	0
$(A^3B^3C^4D^2)_1$	0302 + 3040 + 0324 + 3002 + 0340 + 3024	1
$(A^3B^3C^4D^2)_2$	0004 + 3342 + 0020 + 3304 + 0042 + 3320	2
$(A^3B^3C^4D^2)_3$	0300 + 3044 + 0322 + 3000 + 0344 + 3022	3
$(A^3B^3C^4D^2)_4$	0002 + 3340 + 0024 + 3302 + 0040 + 3324	4
$(A^3B^3C^4D^2)_5$	0304 + 3042 + 0320 + 3004 + 0342 + 3020	5

latin square of order 6

0	5	4	3	2	1
1	0	5	4	3	2
2	1	0	5	4	3
3	2	1	0	5	4
4	3	2	1	0	5
5	4	3	2	1	0

Thus, the above square is simply a column permutation of the previous one. As there are no other sets of 5 degrees of freedom leading to a latin square of order 6 (i.e. A^3, B^3, and A^3B^3 exhaust the three single degrees of freedom from the 2^2 factorial and C^4, D^4, C^4D^4, and C^4D^2 exhaust all sets of 2 degrees of freedom from the 3^2 factorial.), it is not possible to obtain a latin square of order 6 orthogonal to either of the preceding ones using complete confounding schemes.

For a latin square of order 10 we may use levels of $A^5B^5C^6D^6$, $A^5B^5C^6D^2$, $A^5B^5C^6D^8$, or $A^5B^5C^6D^4$ to form four different latin squares of order 10.

II. 2. Partial Confounding

In the last section use was made of complete confounding of effects in a factorial with the rows, columns, and symbols in a latin square. In this section some of the factorial effects will be partially confounded with row (column or symbol) contrasts, i.e. contrasts among levels of an effect will be completely confounded with a subset of the row (column or symbol) contrasts and will be unconfounded with the remaining contrasts, and vice versa. In complete confounding no subset of contrasts among the levels of a factorial effect can be separated from contrasts among the rows (columns or symbols). (See, e.g., Yates [1937] and Federer [1955]). For example, the latin square of order 4 could be considered as a 2^4 factorial as in the preceding section, with the following scheme of confounding:

Columns

Rows	1 = $(C)_0$	2 = $(C)_1$	3 = $(D)_0$	4 = $(D)_1$
1 $(A)_0,(B)_0$	0000	0011	0010	0001
2 $(A)_0,(B)_1$	0101	0110	0100	0111
3 $(A)_1,(B)_0$	1000	1011	1010	1001
4 $(A)_1,(B)_1$	1101	1110	1100	1111

If we set up the latin square symbols for the above as

α	β	γ	δ
β	α	δ	γ
γ	δ	β	α
δ	γ	α	β

then

the symbols correspond to the following combinations:

α: $0000 + 0110 + 1001 + 1100 = (ABCD)_0$ + other effects

β: $0011 + 0101 + 1010 + 1111 = (ABCD)_0$ + " "

γ: $1000 + 1110 + 0010 + 0111 = (ABCD)_1$ + " "

δ: $0001 + 0100 + 1011 + 1101 = (ABCD)_1$ + " "

It is known that this latin square has no orthogonal mate (Hedayat [1969]). This means that no orthogonal partition of the remaining sum of squares can be made which forms a latin square.

If on the other hand, the latin square used is

α	β	γ	δ
β	α	δ	γ
γ	δ	α	β
δ	γ	β	α

, the combinations

corresponding to the Greek letters are:

α: $0000 + 0110 + 1010 + 1111 = (ABCD)_0$ + other effects

β: $0011 + 0101 + 1001 + 1100 = (ABCD)_0$ + " "

γ: $0010 + 0111 + 1000 + 1110 = (ABCD)_1 + (AC)_1$ + other effects

δ: $0001 + 0100 + 1011 + 1101 = (ABCD)_1$ + other effects

This square has two mutually orthogonal mates and hence there must be partitions of the sums of squares into orthogonal components which correspond to the symbols in a latin square.

Instead of inserting symbols in the latin square of order 4, denote the symbols in the latin square by the following partial confounding scheme, where a fractional replicate is a subset of a complete factorial:

i) add the two 1/8 replicates generated by $((A)_0, (D)_0, (BC)_0)$ and $((A)_1, (C)_1, (ABD)_1)$ to obtain the 4 combinations (0000 + 0110) + (1010 + 1111) and denote these 4 combinations as symbol α,

ii) add the two 1/8 replicates generated by $((D)_1, (AB)_1, (AC)_0)$ and $((AB)_0, (C)_0, (AD)_1)$ to obtain combinations (0101 + 1011) + (1100 + 0001) and denote these 4 combinations as symbol β,

iii) add the two 1/8 replicates generated by $((A)_1, (D)_0, (ABC)_1)$ and $((A)_0, (C)_1, (BD)_0)$ to obtain combinations (1000 + 1110) + (0010 + 0111) and denote these 4 as symbol γ,

iv) add the two 1/8 replicates generated by $((AB)_0, (AC)_1, (D)_1)$ and $((AB)_1, (C)_0, (BD)_1)$ to obtain the combinations (1101 + 0011) + (0100 + 1001) and denote these 4 as symbol δ.

This procedure results in the following latin square of order 4:

α	δ	γ	β
β	α	δ	γ
γ	β	α	δ
δ	γ	β	α

.

Obviously, one could take any pair of 1/8 replicates such that the 4 combinations are in different rows and in different columns to form the combinations for a given symbol.

The above type of partial confounding results in the class of latin squares denoted as half-plaid latin squares (See Federer [1955] chapters IX and XV and Yates [1937]). If partial confounding were utilized in rows as well as in columns the resulting square would be denoted as a plaid latin square (so-called because of its resemblence to plaid cloth if the effects confounded were of different colors). The three types of squares are illustrated below for a latin square of order 6 where the factorial effects are as described in statistics books (e.g., Federer [1955]):

Complete confounding of effects

	Columns					
Rows	1 = $(A)_0,(C)_0$	2 = $(A)_0,(C)_1$	3 = $(A)_0,(C)_2$	4 = $(A)_1,(C)_0$	5 = $(A)_1,(C)_1$	6 = $(A)_2,(C)_2$
1 = $(B)_0,(D)_0$	0000	0010	0020	1000	1010	1020
2 = $(B)_0,(D)_1$	0001	0011	0021	1001	1011	1021
3 = $(B)_0,(D)_2$	0002	0012	0022	1002	1012	1022
4 = $(B)_1,(D)_0$	0100	0110	0120	1100	1110	1120
5 = $(B)_1,(D)_1$	0101	0111	0121	1101	1111	1121
6 = $(B)_1,(D)_2$	0102	0112	0122	1102	1112	1122

Partial confounding of effects with columns

	Columns					
Rows	1 = $(C)_0$	2 = $(C)_1$	3 = $(C)_2$	4 = $(CD)_0$	5 = $(CD)_1$	6 = $(CD)_2$
1 = $(B)_0,(D)_0$	0000	0010	0020	1000	1010	1020
2 = $(B)_0,(D)_1$	0001	0011	0021	1021	1001	1011
3 = $(B)_0,(D)_2$	0002	0012	0022	1012	1022	1002
4 = $(B)_1,(D)_0$	1100	1110	1120	0100	0110	0120
5 = $(B)_1,(D)_1$	1101	1111	1121	0121	0101	0111
6 = $(B)_1,(D)_2$	1102	1112	1122	0112	0122	0102

Partial confounding in both rows and columns

Rows	Columns					
	$1 = (C)_0$	$2 = (C)_1$	$3 = (C)_2$	$4 = (CD)_0$	$5 = (CD)_1$	$6 = (CD)_2$
$1 = (D)_0$	00	10	20	00	10	20
$2 = (D)_1$	01	11	21	21	01	11
$3 = (D)_2$	02	12	22	12	22	02
$4 = (CD^2)_0$	00	11	22	00	22	11
$5 = (CD^2)_1$	02	10	21	21	10	02
$6 = (CD^2)_2$	01	12	20	12	01	20

In the last table above only the subscripts for combinations of factors c and d have been inserted. There is some difficulty in inserting subscripts for factors a and b such that these effects are orthogonal to both rows and columns. In any event, this problem requires further study to determine if half-plaid latin squares and plaid latin squares lead to latin squares not of the same type as given by complete confounding. If the three types of latin squares of order 6 can be produced by partial and complete confounding, this would be an interesting result.

III. Fractional Replication Construction of O(n, t) Sets

Any latin square may be considered as an n^{-1} fraction of an n^3 factorial where the rows represent levels of one factor, the columns represent the levels of the second factor, and the symbols in the latin square represent the levels of the third factor. As an illustration, consider the latin square of order 3 where the 9 combinations represent the 1/3 fraction of a 3^3 factorial as follows:

	Columns		
Rows	0	1	2
0	000	012	021
1	102	111	120
2	201	210	222

The above is the 1/3 fraction of a 3^3 corresponding to $(ABC)_{h+i+j=0, \text{mod } 3}$. Since this is a regular fraction we may write out the aliasing structure in this fraction as follows:

$$
\begin{aligned}
&M + ABC \\
&A + AB^2C^2 + BC \\
&B + AB^2C + AC \\
&C + ABC^2 + AB \\
&AB^2 + AC^2 + BC^2
\end{aligned}
$$

where the effects connected with a plus sign are completely confounded with each other. In the above latin square the symbols 0, 1, 2 correspond to the levels of the third factor, c. Now if we set up a second latin square in which the symbols, say α, β, γ, correspond to the levels of AB^2, the resulting square will be orthogonal to the first one. The square corresponding to levels of $(AB^2)_{i+2j, \text{mod } 3}$ is

$$
\begin{aligned}
000 + 111 + 222 &= \alpha \\
021 + 210 + 102 &= \beta \\
201 + 012 + 120 &= \gamma
\end{aligned}
$$

α	γ	β
β	α	γ
γ	β	α

The class of fractional replicates constituted as an n^{-1} fraction of an n^3 factorial becomes an important one to study as it relates to construction of mutually orthogonal latin squares. In particular, all 2^{-3} fractions of a 2^9 and all 3^{-2} fractions of a 3^6 with all possible aliasing structures could produce several sets of mutually orthogonal latin squares. This could have interesting consequences in finite geometry.

The structure of the left-hand set of parameters in an aliasing structure will have a pattern; for example, for $n = 4$, 5, and 7, the patterns are:

$n = 4$	$n = 5$	$n = 7$
$M + ABC$	$M + ABC$	$M + ABC$
A	A	A
B	B	B
C	C	C
AB^2	AB^2	AB^2
AB^3	AB^3	AB^3
	AB^4	AB^4
		AB^5
		AB^6

Note that although ABC was completely confounded with the mean, any one of the other three-factor interaction components AB^uC^v, $u,v = 1,2,\ldots,n-1$ could have been utilized equally well. Also, note that the levels of C corresponding to symbols produce a latin square , and that the levels of effects below the factor B produce a set of $n-1$ mutually orthogonal latin squares.

In general we want to look at all possible n^{-1} fractions of an n^3 factorial, i.e., the subset of $\binom{n^3}{n^2}$ combinations for which the levels of C are the symbols in a latin square and to study their patterns especially for $n = 7,8$, and 9. All possible fractions, or rather all forms of the aliasing structure, could be classified into all types of t mutually orthogonal latin squares, $O(n,t)$ for $t = 1,2,\ldots,n-1$. Perhaps this is the manner in which the geometries of various values

of n can be exhaustively studied. In fractional factorial notation we want to study all possible aliasing patterns for one latin square, for two latin squares, etc. as given by:

$$\begin{pmatrix} M \\ A \\ B \\ C \end{pmatrix} + W\underline{\beta}_0, \quad \begin{pmatrix} M \\ A \\ B \\ C \\ X \end{pmatrix} + W^* \underline{\beta}_0^*, \quad \text{etc.}$$

where $\underline{\beta}_0$ is the $n^2 + n - 2$ vector containing the interaction effect parameters, W is the $4 \times (n^2 + n - 2)$ matrix of aliasing coefficients, X is one of the two factor interaction effects in $\underline{\beta}_0$ corresponding to a column of zero coefficients in W, and $\underline{\beta}_0^*$ and W^* correspond to $\underline{\beta}_0$ and W with the parameter X deleted. For $n = 3$, $\underline{\beta}_0' = (AB, AB^2, AC, AC^2, BC, BC^2, ABC, ABC^2, AB^2C, AB^2C^2)$ and W is equal to

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Since there are three columns containing all zeros X could be either AB^2, AC^2, or BC^2. Selecting X as AB^2, say, there would be no columns in W^* which contain all zeros. Thus, to obtain an O(n, 2) set from a given O(n, 1) set, at least one column in W should be all zeros. Likewise, to obtain an O(n, 3) set from a given O(n, 2) set, at least one column in W^* should contain all zeros.

We now wish to illustrate the use of fractional replication procedures to construct latin squares which are mateless and which have orthogonal mates. To illustrate let us consider the four standard latin squares of order 4 which are (Fisher and Yates [1957]):

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Square I

0	1	2	3
1	3	0	2
2	0	3	1
3	2	1	0

Square II

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Square III

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Square IV

It is known (Hedayat [1969]) that the first three squares are mateless (There is no transversal through 000.) and that the last square belongs to an O(4, 3) set.

Now number the rows as 0, 1, 2, 3 and denote these as levels of the factor a; number the columns as 0, 1, 2, 3, and denote these as levels of factor b, and the symbols in the latin squares by 0, 1, 2, 3, the levels of the factor c . Then, in factorial notation the above 16 combinations form a one-fourth fraction of a 4^3 factorial treatment design. The aliasing scheme for the fractional replicate given as square IV is

$$M + ABC$$
$$A + BC + AB^2C^2 + AB^3C^3$$
$$B + AC + AB^2C + AB^3C$$
$$C + AB + ABC^2 + ABC^3$$

where $u_1 = 1$, 2 means u_2, and 3 means u_3 from GF(4) and where the effects connected with a plus sign are completely confounded with each other. The completion of the remaining two aliasing structures results in the complete aliasing structures for this 4^{-1} fraction of the 4^3 factorial; these two are:

$$AB^2 + AC^3 + BC^2 + AB^3C^2$$
$$AB^3 + AC^2 + BC^3 + AB^2C^3$$

If we use the levels of AB^2 and of AB^3 to form two latin squares, these two with square IV form an $O(4,3)$ set of mutually orthogonal latin squares.

Now, let us return to the set of four standard squares given above and we note that only <u>four</u> combinations in square IV are replaced to obtain squares I, II, and III. These are:

	additional combinations	combinations replaced in IV
Square I	112, 130, 310, 332	110, 132, 312, 330
" II	113, 120, 210, 223	110, 123, 213, 220
" III	213, 230, 320, 331	220, 231, 321, 330

The aliasing structure (without the coefficients) is given on the following page for all four standard latin squares of order 4. The 1/4 replicate given by square IV forms a regular fraction. The remaining three fractional replicates are such that <u>none</u> of the additional effects are <u>unconfounded</u> with the effects M, A, B, or C of the original latin squares of order 4. Since this is true no linear combination of these effects will be unconfounded. In order to form a latin square which is orthogonal to the given one it is necessary that there be a set of effects which is unconfounded with the effects in the given square. This is impossible for the three squares I, II, and III and hence the squares are mateless, as is well-known.

It would be interesting to ascertain the aliasing structures for the six standard latin squares of order 5 belonging to the $O(5,4)$ set and for the fifty standard latin squares of order 5 for which are known to be mateless (Hedayat

Aliasing structure of effects in the four 1/4 fractional replicates of a 4^3 factorial for four standard latin squares of order 4

	Square I				Square II				Square III				Square IV			
	Effect				Effect				Effect				Effect			
Effect	mean = M	rows = A	cols. = B	letters = C	mean = M	rows = A	cols. = B	letters = C	mean = M	rows = A	cols. = B	letters = C	mean = M	rows = A	cols. = B	letters = C
M	-				-				-				-			
A		-				-				-				-		
B			-				-				-				-	
C				-				-				-				-
AB				P				P				P				C
AB^2				P				P				P				
AB^3				P				P				P				
AC			P				P				P				C	
AC^2			P				P				P					
AC^3			P				P				P					
BC		P				P				P				C		
BC^2		P				P				P						
BC^3		P				P				P						
ABC	P	P	P	P	P	P	P	P		P	P	P	C			
ABC^2	P	P	P	P	P	P	P	P	P	P	P	P				C
ABC^3	P	P	P	P	P	P	P	P	P	P	P	P				C
AB^2C	P	P	P	P	P	P	P	P	P	P	P	P			C	
AB^2C^2	P	P	P	P	P	P	P	P	P	P	P	P		C		
AB^2C^3	P	P	P	P		P	P	P		P	P	P				
AB^3C	P	P	P	P	P	P	P	P	P	P	P	P			C	
AB^3C^2		P	P	P		P	P	P		P	P	P				
AB^3C^3	P	P	P	P	P	P	P	P	P	P	P	P		C		
No. of effects confounded with	8	12	12	12	7	12	12	12	6	12	12	12	1	3	3	3

- means identical effect
C means complete confounding
P means partial confounding
blank means unconfounded

$$AB^2 + AC^3 + BC^2 + AB^3C^2$$
$$AB^3 + AC^2 + BC^3 + AB^2C^3$$

If we use the levels of AB^2 and of AB^3 to form two latin squares, these two with square IV form an $O(4, 3)$ set of mutually orthogonal latin squares.

Now, let us return to the set of four standard squares given above and we note that only four combinations in square IV are replaced to obtain squares I, II, and III. These are:

	additional combinations	combinations replaced in IV
Square I	112, 130, 310, 332	110, 132, 312, 330
" II	113, 120, 210, 223	110, 123, 213, 220
" III	213, 230, 320, 331	220, 231, 321, 330

The aliasing structure (without the coefficients) is given on the following page for all four standard latin squares of order 4. The 1/4 replicate given by square IV forms a regular fraction. The remaining three fractional replicates are such that none of the additional effects are unconfounded with the effects M, A, B, or C of the original latin squares of order 4. Since this is true no linear combination of these effects will be unconfounded. In order to form a latin square which is orthogonal to the given one it is necessary that there be a set of effects which is unconfounded with the effects in the given square. This is impossible for the three squares I, II, and III and hence the squares are mateless, as is well-known.

It would be interesting to ascertain the aliasing structures for the six standard latin squares of order 5 belonging to the $O(5, 4)$ set and for the fifty standard latin squares of order 5 for which are known to be mateless (Hedayat

Aliasing structure of effects in the four 1/4 fractional replicates of a 4^3 factorial for four standard latin squares of order 4

	Square I				Square II				Square III				Square IV			
	Effect				Effect				Effect				Effect			
Effect	mean = M	rows = A	cols. = B	letters = C	mean = M	rows = A	cols. = B	letters = C	mean = M	rows = A	cols. = B	letters = C	mean = M	rows = A	cols. = B	letters = C
M	-				-				-				-			
A		-				-				-				-		
B			-				-				-				-	
C				-				-				-				-
AB				P				P				P				C
AB^2				P				P				P				
AB^3				P				P				P				
AC			P				P				P				C	
AC^2			P				P				P					
AC^3			P				P				P					
BC		P				P				P				C		
BC^2		P				P				P						
BC^3		P				P				P						
ABC	P	P	P	P	P	P	P	P		P	P	P	C			
ABC^2	P	P	P	P	P	P	P	P	P	P	P	P				C
ABC^3	P	P	P	P	P	P	P	P	P	P	P	P				C
AB^2C	P	P	P	P	P	P	P	P	P	P	P	P			C	
AB^2C^2	P	P	P	P	P	P	P	P	P	P	P	P		C		
AB^2C^3	P	P	P	P		P	P	P		P	P	P				
AB^3C	P	P	P	P	P	P	P	P	P	P	P	P			C	
AB^3C^2		P	P	P		P	P	P		P	P	P				
AB^3C^3	P	P	P	P	P	P	P	P	P	P	P	P		C		
No. of effects confounded with	8	12	12	12	7	12	12	12	6	12	12	12	1	3	3	3

\- means identical effect C means complete confounding

P means partial confounding blank means unconfounded

[1969]). After a study of these fractions, one should continue such a study for $n = 7$, 8, and 9. It is suggested that one consider a 2^{6-2} fraction instead of a 4^{3-1} fraction for $n = 4$ and a 2^{9-3} fraction instead of an 8^{3-1} fraction for $n = 8$. The reason for this is that there is much more theory available for $s = 2$ in the s^m series than for any other value of s. Also, one may use the generalized defining contrast which has been developed by Raktoe and Federer [1969] to a considerable advantage in writing out aliasing structures in these cases. Investigation of the regular and irregular fractional replicates obtainable for various values of n could lead to considerable advances in the theory of mutually orthogonal latin squares.

IV. ANOVA Construction of O(n, t) Sets

There should be some procedure which would utilize the orthogonality of single degree of freedom contrasts in the analysis of variance (ANOVA) and which could be utilized to construct orthogonal latin squares. For example, one could make use of orthogonal polynomial coefficients for row and column contrasts and then construct mutually orthogonal latin squares from these. To illustrate, consider the latin square of order 4 used previously wherein the row-column intersections are numbered as a 2^4 factorial, i.e.:

	Column			
Row	1	2	3	4
1	0000	0001	0010	0011
2	0100	0101	0110	0111
3	1000	1001	1010	1011
4	1100	1101	1110	1111

The relation between the 16 contrasts using orthogonal polynomial coefficients and the 2^4 factorial is given below, where R_L, R_Q, and R_C are linear, quadratic, and cubic polynomial contrasts among rows and C_L, C_Q, and C_C are linear, quadratic, and cubic polynomial contrasts among the columns:

Source of variation	df		
C. F. M.	1		
Row contrasts	3		
$A = -R_L - 2R_C$	1	1	Rows linear = $R_L = A + 2B$
$B = -2R_L + R_C$	1	1	" quadratic = $R_Q = AB$
$AB = R_Q$	1	1	" cubic = $R_C = 2A - B$
Column contrasts	3		
$C = -C_L - 2C_C$	1	1	Columns linear = $C_L = C + 2D$
$D = -2C_L + C_C$	1	1	" quadratic = $C_Q = CD$
$CD = C_Q$	1	1	" cubic = $C_C = 2C - D$
Roman numbers = (AB^{u_1})	3		
$AC = R_L C_L + 4R_C C_C$	1	1	$R_L C_L$
$BD = 4R_L C_L + R_C C_C$	1	1	$R_C C_C$
$ABCD = R_Q C_Q$	1	1	$R_Q C_Q$
Greek letters = (AB^{u_2})	3		
$ABD = -2R_Q C_L + R_Q C_C$	1	1	$R_L C_Q$
$BC = 2R_L C_L - 2R_C C_C + 4R_L C_C - R_C C_L$	1	1	$R_Q C_C$
$ACD = (-R_L - 2R_C)C_Q$	1	1	$R_C C_L$
Latin letters = (AB^{u_3})	3		
$AD = 2R_L C_L - 2R_C C_C - R_L C_C + 4R_C C_L$	1	1	$R_L C_C$
$ABC = R_Q(-C_L - 2C_C)$	1	1	$R_Q C_L$
$BCD = (-2R_L + R_C)C_Q$	1	1	$R_C C_Q$
Total	16		

The individual degree of freedom contrast matrix for the above 16 combination is:

Contrast	Combination 0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Mean	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
R_L	-3	-3	-3	-3	-	-	-	-	+	+	+	+	3	3	3	3
R_Q	+	+	+	+	-	-	-	-	-	-	-	-	+	+	+	+
R_C	+	+	+	+	-3	-3	-3	-3	3	3	3	3	-	-	-	-
C_L	-3	-	+	3	-3	-	+	3	-3	-	+	3	-3	-	+	3
C_Q	+	-	-	+	+	-	-	+	+	-	-	+	+	-	-	+
C_C	+	-3	3	-	+	-3	3	-	+	-3	3	-	+	-3	3	-
R_LC_L	9	3	-3	-9	3	+	-	-3	-3	-	+	3	-9	-3	3	9
R_LC_Q	-3	3	3	-3	-	+	+	-	+	-	-	+	3	-3	-3	3
R_LC_C	-3	9	-9	3	-	3	-3	+	+	-3	3	-	3	-9	9	-3
R_QC_L	-3	-	+	3	3	+	-	-3	3	+	-	-3	-3	-	+	3
R_QC_Q	+	-	-	+	-	+	+	-	-	+	+	-	+	-	-	+
R_QC_C	+	-3	3	-	-	3	-3	+	-	3	-3	+	+	-3	3	-
R_CC_L	-3	-	+	3	9	3	-3	-9	-9	-3	3	9	3	+	-	-3
R_CC_Q	+	-	-	+	-3	3	3	-3	3	-3	-3	3	-	+	+	-
R_CC_C	+	-3	3	-	-3	9	-9	3	3	-9	9	-3	-	3	-3	+

The corresponding single degree of freedom contrast matrix for the 2^4 factorial is:

Source of variation	df		
C. F. M.	1		
Row contrasts	3		
$A = -R_L - 2R_C$	1	1	Rows linear = $R_L = A + 2B$
$B = -2R_L + R_C$	1	1	" quadratic = $R_Q = AB$
$AB = R_Q$	1	1	" cubic = $R_C = 2A - B$
Column contrasts	3		
$C = -C_L - 2C_C$	1	1	Columns linear = $C_L = C + 2D$
$D = -2C_L + C_C$	1	1	" quadratic = $C_Q = CD$
$CD = C_Q$	1	1	" cubic = $C_C = 2C - D$
Roman numbers = (AB^{u_1})	3		
$AC = R_L C_L + 4R_C C_C$	1	1	$R_L C_L$
$BD = 4R_L C_L + R_C C_C$	1	1	$R_C C_C$
$ABCD = R_Q C_Q$	1	1	$R_Q C_Q$
Greek letters = (AB^{u_2})	3		
$ABD = -2R_Q C_L + R_Q C_C$	1	1	$R_L C_Q$
$BC = 2R_L C_L - 2R_C C_C + 4R_L C_C - R_C C_L$	1	1	$R_Q C_C$
$ACD = (-R_L - 2R_C) C_Q$	1	1	$R_C C_L$
Latin letters = (AB^{u_3})	3		
$AD = 2R_L C_L - 2R_C C_C - R_L C_C + 4R_C C_L$	1	1	$R_L C_C$
$ABC = R_Q(-C_L - 2C_C)$	1	1	$R_Q C_L$
$BCD = (-2R_L + R_C) C_Q$	1	1	$R_C C_Q$
Total	16		

The individual degree of freedom contrast matrix for the above 16 combination is:

Contrast	Combination															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Mean	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
R_L	-3	-3	-3	-3	-	-	-	-	+	+	+	+	3	3	3	3
R_Q	+	+	+	+	-	-	-	-	-	-	-	-	+	+	+	+
R_C	+	+	+	+	-3	-3	-3	-3	3	3	3	3	-	-	-	-
C_L	-3	-	+	3	-3	-	+	3	-3	-	+	3	-3	-	+	3
C_Q	+	-	-	+	+	-	-	+	+	-	-	+	+	-	-	+
C_C	+	-3	3	-	+	-3	3	-	+	-3	3	-	+	-3	3	-
R_LC_L	9	3	-3	-9	3	+	-	-3	-3	-	+	3	-9	-3	3	9
R_LC_Q	-3	3	3	-3	-	+	+	-	+	-	-	+	3	-3	-3	3
R_LC_C	-3	9	-9	3	-	3	-3	+	+	-3	3	-	3	-9	9	-3
R_QC_L	-3	-	+	3	3	+	-	-3	3	+	-	-3	-3	-	+	3
R_QC_Q	+	-	-	+	-	+	+	-	-	+	+	-	+	-	-	+
R_QC_C	+	-3	3	-	-	3	-3	+	-	3	-3	+	+	-3	3	-
R_CC_L	-3	-	+	3	9	3	-3	-9	-9	-3	3	9	3	+	-	-3
R_CC_Q	+	-	-	+	-3	3	3	-3	3	-3	-3	3	-	+	+	-
R_CC_C	+	-3	3	-	-3	9	-9	3	3	-9	9	-3	-	3	-3	+

The corresponding single degree of freedom contrast matrix for the 2^4 factorial is:

The corresponding single degree of freedom contrast matrix for the 2^4 factorial is:

Contrast	Combination															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Mean	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
A	−	−	−	−	−	−	−	−	+	+	+	+	+	+	+	+
B	−	−	−	−	+	+	+	+	−	−	−	−	+	+	+	+
AB	+	+	+	+	−	−	−	−	−	−	−	−	+	+	+	+
C	−	−	+	+	−	−	+	+	−	−	+	+	−	−	+	+
D	−	+	−	+	−	+	−	+	−	+	−	+	−	+	−	+
CD	+	−	−	+	+	−	−	+	+	−	−	+	+	−	−	+
AC	+	−	+	−	+	−	+	−	−	+	−	+	−	+	−	+
BD	+	−	−	+	−	+	−	+	+	−	+	−	−	+	−	+
ABCD	−	+	+	−	−	+	+	−	−	+	+	−	−	+	+	−
ABD	−	+	+	−	+	−	−	+	−	+	+	−	+	−	−	+
BC	+	−	−	+	+	−	−	+	−	+	+	−	−	+	+	−
ACD	+	+	−	−	−	−	+	+	−	−	+	+	−	−	+	+
ABC	+	+	−	−	+	+	−	−	+	+	−	−	+	+	−	−
AD	−	+	−	+	+	−	+	−	+	−	+	−	−	+	−	+
BCD	−	−	+	+	+	+	−	−	−	−	+	+	+	+	−	−

The particular contrast matrix utilized is not unique, as has been demonstrated above. All orthogonal contrast matrices resulting in latin squares could be considered. For example, other sets of contrasts among rows (or columns) could be:

	1	2	3	4
Mean	+	+	+	+
R_1	-	+	0	0
R_2	0	0	-	+
R_3	+	+	-	-

or

	1	2	3	4
Mean	+	+	+	+
R_1	-	+	0	0
R_2	+	+	-2	0
R_3	+	+	+	-3

The interaction of row and column contrasts possibly could be utilized to allocate the symbols in the latin square.

We wish to illustrate the method of constructing latin squares using orthogonal polynomial coefficients. We shall first consider the construction of three mutually orthogonal latin squares of order 4 and then we shall consider the construction of a single latin square of order 6. In the preceding table on orthogonal polynomials for $n = 4$ denote all combinations with a plus sign as belonging to $(R_L C_L)_1$ and those with a minus sign as belonging to $(R_L C_L)_0$. Do likewise for the $R_Q C_Q$ and $R_C C_C$ effects. Then, the four latin square symbols are obtained as follows:

$$(R_L C_L)_1, (R_Q C_Q)_1, (R_C C_C)_1 = 0000 + 0101 + 1010 + 1111 = A$$

$$(R_L C_L)_1, (R_Q C_Q)_0, (R_C C_C)_0 = 0001 + 0100 + 1011 + 1110 = B$$

$$(R_L C_L)_0, (R_Q C_Q)_0, (R_C C_C)_1 = 0010 + 0111 + 1000 + 1101 = C$$

$$(R_L C_L)_0, (R_Q C_Q)_1, (R_C C_C)_0 = 0011 + 0110 + 1001 + 1100 = D$$

This results in the following latin square of order 4

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

Likewise, if we use the following polynomial contrasts we obtain the two mutually orthogonal mates of the above square:

$$(R_L C_Q)_1,\ (R_Q C_C)_0,\ (R_C C_L)_0 = 0001 + 0110 + 1000 + 1111 = \alpha$$
$$(R_L C_Q)_1,\ (R_Q C_C)_1,\ (R_C C_L)_1 = 0010 + 0101 + 1011 + 1100 = \beta$$
$$(R_L C_Q)_0,\ (R_Q C_C)_0,\ (R_C C_L)_1 = 0011 + 0100 + 1010 + 1101 = \gamma$$
$$(R_L C_Q)_0,\ (R_Q C_C)_1,\ (R_C C_L)_0 = 0111 + 1001 + 1110 + 0000 = \delta$$

and

$$(R_L C_C)_1,\ (R_Q C_L)_1,\ (R_C C_Q)_1 = 0011 + 0101 + 1000 + 1110 = I$$
$$(R_L C_C)_1,\ (R_Q C_L)_0,\ (R_C C_Q)_0 = 0001 + 0111 + 1010 + 1100 = II$$
$$(R_L C_C)_0,\ (R_Q C_L)_0,\ (R_C C_Q)_1 = 0000 + 0110 + 1011 + 1101 = III$$
$$(R_L C_C)_0,\ (R_Q C_L)_1,\ (R_C C_Q)_0 = 0010 + 0100 + 1001 + 1111 = IV$$

The above results in the following two latin squares of order 4

δ	α	β	γ
γ	β	α	δ
α	δ	γ	β
β	γ	δ	α

III	II	IV	I
IV	I	III	II
I	IV	II	III
II	III	I	IV

The above method of constructing mutually orthogonal latin squares using polynomial coefficients works for latin squares of order n where $n = 2^p$. We need another procedure for other values of n and shall now construct a latin square of order 6 from the orthogonal polynomial coefficients in the table of single degree of freedom contrasts for 36 combinations. If we observe only the signs of contrasts we note that the 36 combinations may be classified into

six sets of four with like signs and two additional sets of six. The latter two sets will be used to build up the six sets of four into six sets of six as follows where all combinations with a plus sign go in the one level and all those with a minus sign go in the zero level (see page 32):

$(R_2C_2)_1, (R_3C_3)_1, (R_4C_4)_0, (R_5C_5)_0$ + 2 from $(R_1C_1)_1, (R_2C_2)_1 (R_3C_3)_1, (R_4C_4)_1, (R_5C_5)_1$
$(R_2C_2)_0, (R_3C_3)_0, (R_3C_4)_1 (R_5C_5)_0$ + "
$(R_2C_2)_0, (R_3C_3)_0, (R_4C_4)_0, (R_5C_5)_0$ + "
$(R_2C_2)_0, (R_3C_3)_1, (R_4C_4)_0, (R_5C_5)_1$ + 2 from $(R_1C_1)_0, (R_2C_2)_1, (R_3C_3)_0, (R_4C_4)_1, (R_5C_5)_0$
$(R_2C_2)_0, (R_3C_3)_1, (R_4C_4)_1, (R_5C_5)_0$ + "
$(R_2C_2)_1, (R_3C_3)_0, (R_4C_4)_0, (R_5C_5)_1$ + "

From these sets we obtain

(12 + 21 + 34 + 43) + (00 + 55) = A
(02 + 20+ 35 + 53) + (11 + 44) = B
(01 + 10 +45 +54) + (22 + 33) = C
(04 + 15 +40 + 51) + (23 + 32) = D
(03 + 25 +30 + 52) + (14 + 41) = E
(13 + 24 +31 + 42) + (05 + 50) = F

This results in the following latin square of order 6:

00 A	10 C	20 B	30 E	40 D	50 F
01 C	11 B	21 A	31 F	41 E	51 D
02 B	12 A	22 C	32 D	42 F	52 E
03 E	13 F	23 D	33 C	43 A	53 B
04 D	14 E	24 F	34 A	44 B	54 C
05 F	15 D	25 E	35 B	45 C	55 A

The pair of treatments in the second set of parentheses, e.g. (00 + 55), was picked from the set of six in such a manner as to have i and j in the combination ij, contain 0, 1, 2, 3, 4, and 5 since each letter must appear once in each row and once in each column.

It would be interesting and perhaps enlightening to carry out the above procedure for n = 10 and 12 and to exhaustively study the complete set of 35 contrasts for n = 6 .

	00	01	02	03	04	05	10	11	12	13	14	15	20	21	22	23	24	25	30	31	32	33	34	35	40	41	42	43	44	45	50	51	52	53	54	55
R_1	-5	-5	-5	-5	-5	-5	-3	-3	-3	-3	-3	-3	-1	-1	-1	-1	-1	-1	1	1	1	1	1	1	3	3	3	3	3	3	5	5	5	5	5	5
R_2	5	5	5	5	5	5	-1	-1	-1	-1	-1	-1	-4	-4	-4	-4	-4	-4	-4	-4	-4	-4	-4	-4	-1	-1	-1	-1	-1	-1	5	5	5	5	5	5
R_3	-5	-5	-5	-5	-5	-5	7	7	7	7	7	7	4	4	4	4	4	4	-4	-4	-4	-4	-4	-4	-7	-7	-7	-7	-7	-7	5	5	5	5	5	5
R_4	1	1	1	1	1	1	-3	-3	-3	-3	-3	-3	2	2	2	2	2	2	2	2	2	2	2	2	-3	-3	-3	-3	-3	-3	1	1	1	1	1	1
R_5	-1	-1	-1	-1	-1	-1	5	5	5	5	5	5	-10	-10	-10	-10	-10	-10	10	10	10	10	10	10	-5	-5	-5	-5	-5	-5	1	1	1	1	1	1
C_1	-5	-3	-1	1	3	5	-5	-3	-1	1	3	5	-5	-3	-1	1	3	5	-5	-3	-1	1	3	5	-5	-3	-1	1	3	5	-5	-3	-1	1	3	5
C_2	5	-1	-4	-4	-1	5	5	-1	-4	-4	-1	5	5	-1	-4	-4	-1	5	5	-1	-4	-4	-1	5	5	-1	-4	-4	-1	5	5	-1	-4	-4	-1	5
C_3	-5	7	4	-4	-7	5	-5	7	4	-4	-7	5	-5	7	4	-4	-7	5	-5	7	4	-4	-7	5	-5	7	4	-4	-7	5	-5	7	4	-4	-7	5
C_4	1	-3	2	2	-3	1	1	-3	2	2	-3	1	1	-3	2	2	-3	1	1	-3	2	2	-3	1	1	-3	2	2	3	1	1	-3	2	2	-3	1
C_5	-1	5	-10	10	-5	1	-1	5	-10	10	-5	1	-1	5	-10	10	-5	1	-1	5	-10	10	-5	1	-1	5	-10	10	-5	1	-1	5	-10	10	-5	1
R_1C_1	25	15	5	-5	-15	-25	15	9	3	-3	-9	-15	5	3	1	-1	-3	-5	-5	-3	-1	1	3	5	-15	-9	-3	3	9	15	-25	-15	-5	5	15	25
R_2C_2	25	-5	-20	-20	-5	25	-5	1	4	4	1	-5	-20	4	16	16	4	-20	-20	4	16	16	4	-20	-5	1	4	4	1	-5	25	-5	-20	-20	-5	25
R_3C_3	25	-35	-20	20	35	-25	-35	49	28	-28	-49	35	-20	28	16	-16	-28	20	20	-28	-16	16	28	-20	35	-49	-28	28	49	-35	-25	35	20	-20	-35	25
R_4C_4	1	-3	2	2	-3	1	-3	9	-6	-6	9	-3	2	-6	4	4	-6	2	2	-6	4	4	-6	2	-3	9	-6	-6	9	-3	1	-3	2	2	-3	1
R_5C_5	1	-5	10	-10	5	-1	-5	25	-50	50	-25	5	10	-50	100	-100	50	-10	-10	50	-100	100	-50	10	5	-25	50	-50	25	-5	-1	5	-10	10	-5	1

V. Group Construction of O(n, t) Sets

V.0. Introduction

The construction of $O(n,t)$ sets based on groups and their associated mappings such as automorphism, complete mapping, and orthomorphism is the oldest and still the most popular method for n not of the form $4t + 2$. Euler [1782] implicitly utilized some properties of finite groups of order $2t + 1$ and $4t$ for his construction of $O(2t+1,2)$ and $O(4t,2)$ sets, respectively. It was MacNeish [1922] who, for the first time, explicitly (however, not rigorously) utilized group properties for his construction of $O(q^m, q^m-1)$ sets and $O(n, \lambda)$ sets, where q is a prime, m is a positive integer and if $n = q_1^{\ell_1} q_2^{\ell_2} \ldots q_r^{\ell_r}$ is the prime power decomposition of n then $\lambda = \min(q_1^{\ell_1}, q_2^{\ell_2}, \ldots, q_r^{\ell_r})-1$. The field construction of $O(q^m, q^m - 1)$ sets found independently by Bose [1938] and Stevens [1939] is based on the additive group of $GF(q^m)$ and its related cyclic group of automorphisms. The $O(n,n-1)$ sets for $n = 3,4,5,7,8$ and 9 exhibited by Fisher and Yates [1957] are based on cyclic group and abelian groups. Several beautiful applications of group theory to the existence and non-existence of $O(n,t)$ sets have been found by Mann [1942, 1943, 1944]. The $O(12,5)$ sets found by Johnson et al. [1961] and Bose et al. [1960] are based on abelian groups of order 12. Hedayat [1969] and Hedayat and Federer [1969] have found a series of results on the existence and non-existence of $O(n,t)$ sets through the group theory approach. The reader interested in this subject will find the following references together with the references given to these papers very useful: Paige [1951], Hall-Paige [1955], Singer [1960], Bruck [1951], and Sade [1958].

The author has no doubt that the reader can find many more interesting papers directly or indirectly related to this rich subject.

V.1. Definitions and Notations

There are several forms of definitions of latin squares and orthogonal latin squares. The following forms are useful for the results which will follow:

Definition V.1.1. A latin square of order n on an n-set $\sum$ is an $n \times n$ matrix whose rows and columns are each a permutation of the set $\sum$. Every latin square of order n may therefore be identified with a set of n permutations $(p_1, p_2, \ldots, p_n)$ where p_i is the permutation associated with the ith row.

Definition V.1.2. Let L_i be a latin square of order n on an n-set $\sum_i$, $i = 1,2,\ldots,t$. Then, the set $S = \{L_1, L_2, \ldots, L_t\}$ is said to be a mutually orthogonal set of t latin squares if the projection of the superimposed form of the t latin squares on any two n-sets $\sum_i$ and $\sum_j$, $i \neq j$, forms a permutation of the cartesian product set of $\sum_i$ and $\sum_j$. Such a set is denoted as an $O(n,t)$ set. (See also definitions I.2 and I.3.)

Definition V.1.3. If $L_1 = (P_{11}, P_{12}, \ldots, P_{1n})$ and $L_2 = (P_{21}, P_{22}, \ldots, P_{2n})$ are two latin squares of order n on an n-set $\sum$, then we may define L_1L_2 to be $L_3 = (P_{11}P_{21}, P_{12}P_{22}, \ldots, P_{1n}P_{2n})$ (see definition V.1.1). The generalization to the product of $t > 2$ latin squares follows immediately.

V.2. Construction of $O(n,t)$ Sets Based on a Group

We shall divide the problem into three parts based on whether n is a prime, or a mixture of prime powers. The proof of the subsequent results can be found in the references related to this section.

V. 2. 1. n = q a prime. Recall that any prime ordered group is cyclic.

Theorem V. 2. 1. 1. Let $G = \{P_1, P_2, \ldots, P_q\}$ be a cyclic permutation group of degree q and order q. Then, $S_{11} = \{L_1, L_2, \ldots, L_{q-1}\}$ is an O(q, q-1) set, where $L_i = (P_1^i, P_2^i, \ldots, P_q^i)$.

Demonstration V. 2. 1. 1. Let q = 5. Select any arbitrary generator such as $\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}$ which generates a cyclic permutation group G and, hence, a latin square L_1. Then,

$L_1 =$

3	5	2	1	4
2	4	5	3	1
5	1	4	2	3
4	3	1	5	2
1	2	3	4	5

, $L_2 =$

2	4	5	3	1
4	3	1	5	2
3	5	2	1	4
5	1	4	2	3
1	2	3	4	5

, $L_3 =$

5	1	4	2	3
3	5	2	1	4
4	3	1	5	2
2	4	5	3	1
1	2	3	4	5

, $L_4 =$

4	3	1	5	2
5	1	4	2	3
2	4	5	3	1
3	5	2	1	4
1	2	3	4	5

For those who do not like to work with permutation groups we present the following theorem:

Theorem V. 2. 1. 2. Let L(r) be an n × n square with ri + j (mod q) in its (i, j)th cell, i, j = 0, 1, . . . , q-1. Then, $S_{12} = \{L(1), L(2), \ldots, L(q-1)\}$ is an O(q, q-1) set if q is a prime.

Demonstration V. 2. 1. 2. Let q = 5; then,

L(1) =

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

, L(2) =

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

, L(3) =

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

, L(4) =

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

Note that $L(1)$ in theorem V.2.1.2 is based on the cyclic permutation group generated by $\begin{pmatrix} 0 & 1 & 2 & \dots & q-1 \\ 1 & 2 & 3 & \dots & 0 \end{pmatrix}$ and $L(i) = L^i(1)$, $i = 2,3,\dots,q-1$. Hence theorem V.2.1.2 is a special case of theorem V.2.1.1.

V.2.2. $n = q^m$ where q is a prime and m any positive integer. Note that this case in particular for $m = 1$ includes case 1. We shall present three theorems for this case. The first two are based on cyclic groups and the third one is based on any group which admits an automorphism of order t.

Theorem V.2.2.1. Let $G = \{P_1, P_2, \dots, P_n\}$ be a cyclic permutation group of degree n and order n. Then, $S_{21} = \{L_1, L_2, \dots, L_\lambda\}$ is an $O(n,\lambda)$ set where $n = q^m$, $\lambda = q-1$, and $L_i = (P_1^i, P_2^i, \dots, P_n^i)$.

Demonstration V.2.2.1. Let $n = 3^2 = 9$. Select any arbitrary generator such as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 1 & 6 & 7 & 8 & 9 & 2 \end{pmatrix}$ which generates a cyclic permutation group G and hence, a latin square L. Then, since $\lambda = 2$,

$L_1 =$

3	4	5	1	6	7	8	9	2
5	1	6	3	7	8	9	2	4
6	3	7	5	8	9	2	4	1
7	5	8	6	9	2	4	1	3
8	6	9	7	2	4	1	3	5
9	7	2	8	4	1	3	5	6
2	8	4	9	1	3	5	6	7
4	9	1	2	3	5	6	7	8
1	2	3	4	5	6	7	8	9

and $L_2 =$

5	1	6	3	7	8	9	2	4
7	5	8	6	9	2	4	1	3
9	7	2	8	4	1	3	5	6
4	9	1	2	3	5	6	7	8
3	4	5	1	6	7	8	9	2
6	3	7	5	8	9	2	4	1
8	6	9	7	2	4	1	3	5
2	8	4	9	1	3	5	6	7
1	2	3	4	5	6	7	8	9

is an $O(9,2)$ set.

Conjecture. The set S_{21} is orthogonally locked, meaning that there does not exist a latin square L^* such that $S_{21} \cup \{L^*\}$ is an $O(n,\lambda+1)$ set.

Note that for n even this conjecture is correct since any latin square of even order based on cyclic permutation group is orthogonally mateless.

An analogous theorem to theorem V.2.1.2 for this case is:

Theorem V.2.2.2. Let L(r) be an $n \times n$ square with $ri + j \pmod n$ in its (i,j) cell, $i = 0,1,2,\ldots,n-1$. Then $S_{22} = \{L(1), L(2), \ldots, L(\lambda)\}$ is an $O(n,\lambda)$ set if $n = q^m$ and $\lambda = q-1$.

Demonstration V.2.2.2. Let $n = q = 3^2$ then,

$L(1) =$

0	1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8	0
2	3	4	5	6	7	8	0	1
3	4	5	6	7	8	0	1	2
4	5	6	7	8	0	1	2	3
5	6	7	8	0	1	2	3	4
6	7	8	0	1	2	3	4	5
7	8	0	1	2	3	4	5	6
8	0	1	2	3	4	5	6	7

and $L(2) =$

0	1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	0	1
4	5	6	7	8	0	1	2	3
6	7	8	0	1	2	3	4	5
8	0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	8	0
3	4	5	6	7	8	0	1	2
5	6	7	8	0	1	2	3	4
7	8	0	1	2	3	4	5	6

is an $O(9,2)$ set. Note that theorem V.2.2.2 is a special case of theorem V.2.2.1 viz., L(1) is based on the cyclic permutation group generated by $\begin{pmatrix} 0 & 1 & 2 & \ldots & n-1 \\ 1 & 2 & 3 & \ldots & 0 \end{pmatrix}$ and $L(i) = L^i(1)$, $i = 2,\ldots,\lambda$.

Theorem V.2.2.3. Let $G = \{a_1 = e$ the identity, $a_2, \ldots, a_n\}$ be a group of order n and α an automorphism on G such that $\alpha^i(a_j) \neq a_j$, $1 \leq i \leq t$, $a_j \neq e$.

1) $S = \{L_1, L_2, \ldots, L_t\}$ is an $O(n,t)$ set, where

$L_i =$

e	a_2	$\dots$	a_n
$\alpha^i(a_2)$	$\alpha^i(a_2)a_2$	$\dots$	$\alpha^i(a_2)a_n$
$\alpha^i(a_3)$	$\alpha^i(a_3)a_2$	$\dots$	$\alpha^i(a_3)a_n$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\alpha^i(a_n)$	$\alpha^i(a_n)a_2$	$\dots$	$\alpha^i(a_n)a_n$

$i = 1, 2, \dots, t$.

2) If in particular $t = n-1$, then one can simplify the construction of an $O(n, n-1)$ set from the following key latin square by a cyclic permutation of its last $n-1$ rows.

$L_0 =$

e	$\alpha(x)$	$\alpha^2(x)$	$\dots$	$\alpha^t(x)$
$\alpha(x)$	$\alpha(x)\alpha(x)$	$\alpha(x)\alpha^2(x)$	$\dots$	$\alpha(x)\alpha^t(x)$
$\alpha^2(x)$	$\alpha^2(x)\alpha(x)$	$\alpha^2(x)\alpha^2(x)$	$\dots$	$\alpha^2(x)\alpha^t(x)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\alpha^t(x)$	$\alpha^t(x)\alpha(x)$	$\alpha^t(x)\alpha^2(x)$	$\dots$	$\alpha^t(x)\alpha^t(x)$

for any x in G except the identity element.

We see, therefore, that by means of theorem V. 2. 2. 3 one can construct an $O(n,t)$ set if we can find a group G and an automorphism α of order t . In particular, if $t = n-1$ the whole task of construction reduces to the construction of L_0 as described above. If $n = q^m$ then because every elementary

abelian q-group G of order n admits an automorphism α of order $n-1$, we can construct an $O(q^m, q^m - 1)$ set based on G and α. Here we present a general method of constructing such an automorphism for any $n = q^m$. In particular, we shall exhibit such an automorphism for the following n:

$n = 2^m$, $m = 2, 3, \ldots, 9$

$n = 3^m$, $m = 2, 3, \ldots, 6$

$n = 5^m$, $m = 2, 3, 4$

$n = 7^m$, $m = 2, 3$

$n = 11^2, 13^2, 17^2, 19^2, 23^2, 29^2,$ and 31^2.

This will then perhaps be the largest table that has ever been produced so far for $O(n, n-1)$ sets.

Note that there is no loss of generality if we limit ourselves to the following elementary abelian q-group of order $n = q^m$.

$$G^* = \{(b_1\, b_2 \ldots b_m),\ b_j = 0, 1, 2, \ldots, q-1,\ j = 1, 2, \ldots, m\}.$$

The binary operation on G^* is addition mod q componentwise, viz., $(b_1\, b_2 \ldots b_m) + (b'_1\, b'_2 \ldots b'_m) = (c_1\, c_2 \ldots c_m)$ where $c_i = b_i + b'_i \pmod q$. Note that the elements of G^* are simply the treatment combinations of m factors each at q levels. The reason why we have chosen this particular elementary abelian q-group is that it has a well-known structure to those who are concerned with experiment design construction. Note also that G^* is the direct product of m Galois fields, each of order q.

The generator set for every elementary abelian q-group of order q^m consists of m elements, and for uniformity, we may choose the following ordered

generator set for G^* .

$$g = \{(100 \ldots 0), (01,00 \ldots 0), \ldots (00 \ldots, 010), (00 \ldots 01)\} .$$

Note that the structure of every automorphism α on G^* is completely defined if we know the image of each element of g under α . G^* is a vector space of dimension m over $GF(q)$.

Before proceeding further we need the following well-known result:

Theorem V.2.2.4. Let G be an elementary abelian q-group of order $n = q^m$. Then, Automorphism group of G is isomorphic to the (multiplicative) group of all non-singular $m \times m$ matrices with entries in the field of integers mod q .

The construction of an automorphism of order $n-1$ for G^* is equivalent to the construction of an $m \times m$ matrix A such that $A^{n-1} = I$ but $A^t \neq I$ if t is not a multiple of $n-1$ over the field of integers mod q .

We know from linear algebra that if ϕ is a linear map on a vector space V and if $x \in V$ such that $x \neq 0$ but $\phi(x) = x$, then 1 is an eigenvalue of ϕ. Moreover, if $\{\lambda_1, \lambda_2, \ldots, \lambda_t\}$ is the set of eigenvalues of ϕ, then $\{\lambda_1^s, \lambda_2^s, \ldots, \lambda_t^s\}$ is the set of eigenvalues of ϕ^s. Therefore, for our problem we must find a linear map on G^* with a set of eigenvalues λ_i having the property that for each i, $\lambda_i^s \neq 1 \pmod q$ for all $s = 1,2,\ldots,n-2$ and $\lambda_i^{n-1} = 1$. To do so let F be a $GF(q^m)$ and let β be a generator of the multiplicative cyclic group of $GF(q^m)$, i.e. $\beta^i \neq 1$, $i = 1,2,\ldots,n-2$ while $\beta^{n-1} = 1$. Let $f(x)$ be a monic irreducible polynomial over $GF(q)$ for β . Note that $f(x)$ has degree m . β is sometimes called a primitive root or mark of F . Now, if we let A be the companion matrix for β, then it is easy to see that A has the desired property.

Example

Let us find an automorphism of order 3 for $G^* = \{(00), (01), (10), (11)\}$. It is sufficient, by previous arguments, to find a 2×2 matrix A of order 3 over the field of integer mod 2. Let $GF(2^2) = \{0, 1, \beta, \beta + 1\}$ with the following addition (+) and multiplication (·) tables

+	0	1	β	$\beta + 1$
0	0	1	β	$\beta + 1$
1	1	0	$\beta + 1$	β
β	β	$\beta + 1$	0	1
$\beta + 1$	$\beta + 1$	β	1	0

·	0	1	β	$\beta + 1$
0	0	0	0	0
1	0	1	β	$\beta + 1$
β	0	β	$\beta + 1$	1
$\beta + 1$	0	$\beta + 1$	1	β

Note that β is a primitive root for $GF(2^2)$ and $f(x) = x^2 + x + 1$ is a monic irreducible polynomial for β, since $f(\beta) \equiv 0 \pmod 2$. The companion matrix associated with $f(x)$ is

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

As a check

$$A^2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ over } GF(2), \quad A^3 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

over $GF(2)$.

Let us now determine the image of the ordered generator set $g = \{(10), (01)\}$ under A.

$$Ag = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} (10) \\ (01) \end{bmatrix} = \begin{bmatrix} 0\,(10) + 1\,(01) \\ 1\,(10) + 1\,(01) \end{bmatrix} = \begin{bmatrix} (01) \\ (11) \end{bmatrix} .$$

Therefore, $A(10) = (01)$, $A(01) = (11)$, and since $(11) = (10) + (01)$, $(00) = 2(10) + 2(01)$, we have $A(11) = (10)$, $A(00) = (00)$.

Now, we have a group G^* of order 4 and an automorphism of order 3 on G^*. We can now construct an $O(4,3)$ set. Since $e = (00)$, and if we let $x = (10)$ in theorem V.2.2.3, we obtain:

$L_0 =$

(00)	A(10)	$A^2(10)$	$A^3(10)$
A(10)	A(10) A(10)	A(10) $A^2(10)$	A(10) $A^3(10)$
$A^2(10)$	$A^2(10)A(10)$	$A^2(10)A^2(10)$	$A^2(10)A^3(10)$
$A^3(10)$	$A^3(10)A(10)$	$A^3(10)A^2(10)$	$A^3(10)A^3(10)$

=

(00)	(01)	(11)	(10)
(01)	(00)	(10)	(11)
(11)	(10)	(00)	(01)
(10)	(11)	(01)	(00)

.

The other two latin squares are obtained by a cyclic permutation of the last three rows of L_0. Thus,

$L_1 =$

(00)	(01)	(11)	(10)
(10)	(11)	(01)	(00)
(01)	(00)	(10)	(11)
(11)	(10)	(00)	(01)

(00)	(01)	(11)	(10)
(11)	(10)	(00)	(01)
(10)	(11)	(01)	(00)
(01)	(00)	(10)	(11)

$= L_2$.

To simplify the notation we set (00) = 1, (01) = 2, (11) = 3, (10) = 4 to obtain:

$L_0 =$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

, $L_1 =$

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

, and $L_3 =$

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

.

We are now ready to exhibit a generating matrix of order $n-1 = q^m - 1$ with entries from GF(q) for those n promised before.

n	Generator	Order	n	Generator	Order
2^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	3	2^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$	7
2^4	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	15	2^5	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$	31
2^6	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$	63	2^7	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	127
2^8	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$	255	2^9	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$	511

n	Generator	Order	n	Generator	Order
3^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	8	3^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$	26
3^4	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	80	3^5	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$	242
3^6	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$	728	5^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{bmatrix}$	124
5^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	24	7^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	48
5^4	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3 & 3 & 0 & 3 \end{bmatrix}$	624	11^2	$\begin{bmatrix} 0 & 1 \\ 3 & 3 \end{bmatrix}$	120
7^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{bmatrix}$	342	13^2	$\begin{bmatrix} 0 & 1 \\ 5 & 5 \end{bmatrix}$	168
17^2	$\begin{bmatrix} 0 & 1 \\ 5 & 5 \end{bmatrix}$	288	19^2	$\begin{bmatrix} 0 & 1 \\ 4 & 4 \end{bmatrix}$	360
23^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	528	27^2	$\begin{bmatrix} 0 & 1 \\ 3 & 3 \end{bmatrix}$	728
29^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	840	31^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	960

To shed more light on the given procedure we go through another example. Let $n = 2^3$. Then

$$G^* = \{(000), (001), (010), (011), (100), (101), (110), (111)\}$$

$$g = \{(100), (010), (001)\} \quad \text{and} \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} .$$

$$Ag = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} (100) \\ (010) \\ (001) \end{bmatrix} = \begin{bmatrix} (010) \\ (001) \\ (101) \end{bmatrix} .$$

Let x in theorem V.2.2.3 be (100). Then,

$$A(100) = (010) ,$$

$$A^2(100) = (001) ,$$

$$A^3(100) = (101) ,$$

$$A^4(100) = (111) ,$$

$$A^5(100) = (110) ,$$

$$A^6(100) = (011) , \text{ and}$$

$$A^7(100) = (100) .$$

Therefore, we obtain L_0 as follows:

$L_0 =$

(000)	(010)	(001)	(101)	(111)	(110)	(011)	(100)
(010)	(000)	(011)	(111)	(101)	(100)	(001)	(110)
(001)	(011)	(000)	(100)	(110)	(111)	(010)	(101)
(101)	(111)	(100)	(000)	(010)	(011)	(110)	(001)
(111)	(101)	(110)	(010)	(000)	(001)	(100)	(011)
(110)	(100)	(111)	(011)	(001)	(000)	(101)	(010)
(011)	(001)	(010)	(110)	(100)	(101)	(000)	(111)
(100)	(110)	(101)	(011)	(011)	(010)	(111)	(000)

.

Setting $(000) = 1$, $(010) = 2$, $(001) = 3$, $(101) = 4$, $(111) = 5$, $(110) = 6$, $(011) = 7$, $(100) = 8$, then L_0 in a compact form will be:

$L_0 =$

1	2	3	4	5	6	7	8
2	1	7	5	4	8	3	6
3	7	1	8	6	5	2	4
4	5	8	1	2	7	6	3
5	4	6	2	1	3	8	7
6	8	5	7	3	1	4	2
7	3	2	6	8	4	1	5
8	6	4	3	7	2	5	1

.

Now, we can derive $L_1, L_2, \ldots, L_6$ from L_0 by a cyclic permutation of the last 7 rows of L_0, for example,

$L_1 =$

1	2	3	4	5	6	7	8
8	6	4	3	7	2	5	1
2	1	7	5	4	8	3	6
3	7	1	8	6	5	2	4
4	5	8	1	2	7	6	3
5	4	6	2	1	3	8	7
6	8	5	7	3	1	4	2
7	3	2	6	8	4	1	5

, $L_2 =$

1	2	3	4	5	6	7	8
7	3	2	6	8	4	1	5
8	6	4	3	7	2	5	1
2	1	7	5	4	8	3	6
3	7	1	8	6	5	2	4
4	5	8	1	2	7	6	3
6	8	5	7	3	1	4	2
6	8	5	7	3	1	4	2

,

and so on. Note the way L_1 is derived from L_0: except for the first row of L_0 and L_1, which are identical, the i^{th} row of L_0 becomes the $(i+1)^{th}$ row of L_1, and the last row of L_0 becomes the second row of L_1. In general L_j is derived from L_{j-1} in the same fashion as L_1 is derived from L_0.

V.2.3. $n = q_1^{m_1} q_2^{m_2} \ldots q_r^{m_r}$, <u>where</u> q_i <u>is a prime such that</u> $q_i \neq q_j$ if $i \neq j$ <u>and</u> m_i <u>is a positive integer</u>, $i = 1, 2, \ldots, r$.

Theorem V.2.3.1. Let $n = q_1^{m_1} q_2^{m_2} \dots q_r^{m_r}$ be the prime power decomposition of n. Then, there exists an $O(n, \gamma)$ set based on a group, where $\gamma = \min(q_1^{m_1}, q_2^{m_2}, \dots, q_r^{m_r}) - 1$.

Construction. Let $n_i = q_i^{m_i}$. Then, by the method of theorem V.2.2.3 construct an $O(n_i, n_i - 1)$ set $S_i = \{L_{i1}, L_{i2}, \dots, L_{in_i-1}\}$, $i = 1, 2, \dots, r$. Now, let $S_i^* = \{L_{i1}, L_{i2}, \dots, L_{i\gamma}\}$, $i = 1, 2, \dots, r$. Then, $H = \{A_1, A_2, \dots, A_\gamma\}$ is an $O(n, \gamma)$ set where $A_j = L_{1j} \otimes L_{2j} \otimes \dots \otimes L_{rj}$. $\otimes$ denotes the Kronecker product operation.

Demonstration V.2.3.1. Let $n = 12 = 2^2 \cdot 3$. Then, $\gamma = 2$,

$$S_1 = L_{11} = \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array}\ , \quad L_{12} = \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 3&1&2\\\hline 2&3&1\\\hline\end{array}\ ,$$

$$S_2 = L_{21} = \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&1&4&3\\\hline 3&4&1&2\\\hline 4&3&2&1\\\hline\end{array}\ , \quad L_{22} = \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 4&3&2&1\\\hline 2&1&4&3\\\hline 3&4&1&2\\\hline\end{array}\ , \quad L_{23} = \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 3&4&1&2\\\hline 4&3&2&1\\\hline 2&1&4&3\\\hline\end{array}$$

$S_1^* = \{L_{11}, L_{12}\}$ and S_2^* say $\{L_{21}, L_{22}\}$. Then, the reader can easily verify that

$$H = \{A_1 = L_{11} \otimes L_{21},\ A_2 = L_{12} \otimes L_{22}\}$$

is an $O(12, 2)$ set.

Remark. Let n and γ be the same as in theorem V.2.3.1. Then it can be shown that automorphism method fails to produce more than γ mutually orthogonal latin

squares. We shortly show that this inherent defect is due to the mapping not to the group structure.

Definition V. 2. 1. Consider for each positive integer n an abstract group G of order n with binary operation $*$. Let Ω be the collection of all one-to-one mappings of G into itself. Then two maps σ and ψ in Ω are said to be orthogonal if for any g in G,

$$(\sigma Z) * (\psi Z)^{-1} = g$$

has a unique solution Z in G. In particular if σ is an identity map then ψ is said to be an orthomorphism map. A t-subset of Ω is said to be a mutually orthogonal set if every two maps in this t-subset are orthogonal.

Let $L(\cdot)$ be an $n \times n$ square. We make a one-to-one correspondence between the rows of $L(\cdot)$ and the elements of G. Thus, by row x we shall mean the row corresponding to the element x in G. Similarly we make a one-to-one correspondence between the columns of $L(\cdot)$ and the elements of G. The cell of $L(\cdot)$ which occurs in the intersection of row x and column y is called the cell (x,y).

Theorem V. 2. 3. 2. Let σ be in Ω. Put in the cell (x,y) of $L(\cdot)$ the element $(\sigma x) * y$ of G. Call the resulting square $L(\sigma)$. Then $L(\sigma)$ is a latin square of order n on G. Moreover if $\{\sigma_1, \sigma_2, \ldots, \sigma_t\}$ is a set of t mutually orthogonal maps then $\{L(\sigma_1), \ldots, L(\sigma_t)\}$ is an $O(n,t)$ set.

Demonstration V. 2. 3. 2. Let $G = \{0, 1, 2\}$ with the binary operation $x_1 + x_2 = x_3 \pmod 3$, x_i in G. Then the maps σ and ψ with the following definitions are orthogonal.

$$\sigma(0) = 0 \qquad \psi(0) = 0$$
$$\sigma(1) = 1 \qquad \psi(1) = 2$$
$$\sigma(2) = 2 \qquad \psi(2) = 1 \ .$$

The corresponding latin squares to σ and ψ are:

$$L(\sigma) = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 1 & 2 & 0 \\ \hline 2 & 0 & 1 \\ \hline \end{array} \ , \quad L(\psi) = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 2 & 0 & 1 \\ \hline 1 & 2 & 0 \\ \hline \end{array}$$

which are orthogonal.

V. 3. Construction of $O(n,t)$ sets based on t different groups of order n

Up to now we have been concerned with the construction of $O(n,t)$ sets using a group of order n which admits certain mappings. In this section we want to show that for some n's and t's one can construct $O(n,t)$ sets based on t different groups each of order n. This approach proved useful because it lead to the construction of an $O(15, 3)$ set. We should mention that our motivation to search along these lines has stemmed from the following theorem, with a negative flavor, proved by Mann [1944].

Theorem V. 3. 1. It is impossible to construct an $O(5,2)$ set based on two different permutation groups.

For a while we thought that this theorem might be true for all other orders. However, it was found that, fortunately, this is not the case as the following two theorems show:

Theorem V. 3. 2. It is possible to construct $O(7,2)$ sets based on two different cyclic permutation groups of order 7.

Proof: $\{L_1, L_2\}$ is an O(7, 2) set where

$L_1 =$

1	2	3	4	5	6	7
3	7	6	1	4	2	5
6	5	2	3	1	7	4
2	4	7	6	3	5	1
7	1	5	2	6	4	3
5	3	4	7	2	1	6
4	6	1	5	7	3	2

, $L_2 =$

1	2	3	4	5	6	7
2	3	4	5	6	7	1
3	4	5	6	7	1	2
4	5	6	7	1	2	3
5	6	7	1	2	3	4
6	7	1	2	3	4	5
7	1	2	3	4	5	6

.

L_1 and L_2 are based on two different permutation groups as can easily be seen from the different structure of their rows. To be specific L_1 is based on the cyclic permutation group generated by $\begin{pmatrix}1&2&3&4&5&6&7\\3&7&6&1&4&2&5\end{pmatrix}$ and L_2 is based on the cyclic permutation group generated by $\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&5&6&7&1\end{pmatrix}$. Note that, since L_1 and L_2 are based on cyclic permutation groups, then by theorem V. 2. 1. 1 $\{L_1\}$ and $\{L_2\}$ can be embedded in O(7, 6) sets. However, whether or not $\{L_1, L_2\}$ can be embedded in a larger set is an open problem.

Theorem V. 3. 3. It is possible to construct O(15, 3) sets based on three different cyclic permutation groups of order 15.

We remind the reader that every group of order 15 is cyclic.

Proof: $\{L_1, L_2, L_3\}$ is an O(15, 3) set where

L_1 =

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	5	6	7	8	9	10	11	12	13	14	0	1
4	5	6	7	8	9	10	11	12	13	14	0	1	2	3
6	7	8	9	10	11	12	13	14	0	1	2	3	4	5
8	9	10	11	12	13	14	0	1	2	3	4	5	6	7
10	11	12	13	14	0	1	2	3	4	5	6	7	8	9
12	13	14	0	1	2	3	4	5	6	7	8	9	10	11
14	0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
3	4	5	6	7	8	9	10	11	12	13	14	0	1	2
5	6	7	8	9	10	11	12	13	14	0	1	2	3	4
7	8	9	10	11	12	13	14	0	1	2	3	4	5	6
9	10	11	12	13	14	0	1	2	3	4	5	6	7	8
11	12	13	14	0	1	2	3	4	5	6	7	8	9	10
13	14	0	1	2	3	4	5	6	7	8	9	10	11	12

generated by $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 0 & 1 \end{pmatrix}$,

L_2 =

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	11	10	7	9	14	13	6	0	3	4	2	8	5	12
11	2	4	6	3	12	5	13	1	7	9	10	0	14	8
2	10	9	13	7	8	14	5	11	6	3	4	1	12	0
10	4	3	5	6	0	12	14	2	13	7	9	11	8	1
4	9	7	14	13	1	8	12	10	5	6	3	2	0	11
9	3	6	12	5	11	0	8	4	14	13	7	10	1	2
3	7	13	8	14	2	1	0	9	12	5	6	4	11	10
7	6	5	0	12	10	11	1	3	8	14	13	9	2	4
6	13	14	1	8	4	2	11	7	0	12	5	3	10	9
13	5	12	11	0	9	10	2	6	1	8	14	7	4	3
5	14	8	2	1	3	4	10	13	11	0	12	6	9	7
14	12	0	10	11	7	9	4	5	2	1	8	13	3	6
12	8	1	4	2	6	3	9	14	10	11	0	5	7	13
8	0	11	9	10	13	7	3	12	4	2	1	14	6	5

generated by $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 11 & 10 & 7 & 9 & 14 & 13 & 6 & 0 & 3 & 4 & 2 & 8 & 5 & 12 \end{pmatrix}$, and

L_3 =

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
7	4	8	9	11	2	5	12	13	10	0	14	1	3	6
12	11	13	10	14	8	2	1	3	0	7	6	4	9	5
1	14	3	0	6	13	8	4	9	7	12	5	11	10	2
4	6	9	7	5	3	13	11	10	12	1	2	14	0	8
11	5	10	12	2	9	3	14	0	1	4	8	6	7	13
14	2	0	1	8	10	9	6	7	4	11	13	5	12	3
6	8	7	4	13	0	10	5	12	11	14	3	2	1	9
5	13	12	11	3	7	0	2	1	14	6	9	8	4	10
2	3	1	14	9	12	7	8	4	6	5	10	13	11	0
8	9	4	6	10	1	12	13	11	5	2	0	3	14	7
13	10	11	5	0	4	1	3	14	2	8	7	9	6	12
3	0	14	2	7	11	4	9	6	8	13	12	10	5	1
9	7	6	8	12	14	11	10	5	13	3	1	0	2	4
10	12	5	13	1	6	14	0	2	3	9	4	7	8	11

generated by $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 4 & 8 & 9 & 11 & 2 & 5 & 12 & 13 & 10 & 0 & 14 & 1 & 3 & 6 \end{pmatrix}$.

Whether or not $\{L_1, L_2, L_3\}$ can be embedded in an $O(15, t)$, $t > 3$, set is an open problem (see Hedayat [1970]).

V. 4. Concluding Remark

Johnson et al. [1961] and Bose et al. [1960] independently found, by an electronic computer, five mutually orthogonal latin squares by first finding five mutually orthogonal maps for an abelian group of order 12. The $O(12, 5)$ set exhibited below is the set found by Johnson et al. [1961]. Note that the top square is obtained, after a proper renaming, as the direct product of a latin square of order 2 and a cyclic latin square of order 6 being both orthogonally mateless. Moreover, every other square is obtained by proper row permutations, determined by an orthomorphism, from the top square.

Final Remark. The group method fails to produce an $O(n,t)$ set, $t \geq 2$ for any n of the form $4t + 2$. This is so because the Cayley table of any group of order $n = 4t + 2$, which is a latin square of order n, is orthogonally mateless.

0	1	2	3	4	5	6	7	8	9	10	11
5	0	1	2	3	4	11	6	7	8	9	10
4	5	0	1	2	3	10	11	6	7	8	9
3	4	5	0	1	2	9	10	11	6	7	8
2	3	4	5	0	1	8	9	10	11	6	7
1	2	3	4	5	0	7	8	9	10	11	6
6	7	8	9	10	11	0	1	2	3	4	5
11	6	7	8	9	10	5	0	1	2	3	4
10	11	6	7	8	9	4	5	0	1	2	3
9	10	11	6	7	8	3	4	5	0	1	2
8	9	10	11	6	7	2	3	4	5	0	1
7	8	9	10	11	6	1	2	3	4	5	0

0	1	2	3	4	5	6	7	8	9	10	11
6	7	8	9	10	11	0	1	2	3	4	5
10	11	6	7	8	9	4	5	0	1	2	3
4	5	0	1	2	3	10	11	6	7	8	9
11	6	7	8	9	10	5	0	1	2	3	4
5	0	1	2	3	4	11	6	7	8	9	10
9	10	11	6	7	8	3	4	5	0	1	2
7	8	9	10	11	6	1	2	3	4	5	0
2	3	4	5	0	1	8	9	10	11	6	7
8	9	10	11	6	7	2	3	4	5	0	1
1	2	3	4	5	0	7	8	9	10	11	6
3	4	5	0	1	2	9	10	11	6	7	8

0	1	2	3	4	5	6	7	8	9	10	11
3	4	5	0	1	2	9	10	11	6	7	8
6	7	8	9	10	11	0	1	2	3	4	5
5	0	1	2	3	4	11	6	7	8	9	10
9	10	11	6	7	8	3	4	5	0	1	2
7	8	9	10	11	6	1	2	3	4	5	0
4	5	0	1	2	3	10	11	6	7	8	9
10	11	6	7	8	9	4	5	0	1	2	3
1	2	3	4	5	0	7	8	9	10	11	6
2	3	4	5	0	1	8	9	10	11	6	7
11	6	7	8	9	10	5	0	1	2	3	4
8	9	10	11	6	7	2	3	4	5	0	1

0	1	2	3	4	5	6	7	8	9	10	11
10	11	6	7	8	9	4	5	0	1	2	3
5	0	1	2	3	4	11	6	7	8	9	10
7	8	9	10	11	6	1	2	3	4	5	0
1	2	3	4	5	0	7	8	9	10	11	6
9	10	11	6	7	8	3	4	5	0	1	2
3	4	5	0	1	2	9	10	11	6	7	8
8	9	10	11	6	7	2	3	4	5	0	1
4	5	0	1	2	3	10	11	6	7	8	9
11	6	7	8	9	10	5	0	1	2	3	4
6	7	8	9	10	11	0	1	2	3	4	5
2	3	4	5	0	1	8	9	10	11	6	7

0	1	2	3	4	5	6	7	8	9	10	11
2	3	4	5	0	1	8	9	10	11	6	7
7	8	9	10	11	6	1	2	3	4	5	0
8	9	10	11	6	7	2	3	4	5	0	1
4	5	0	1	2	3	10	11	6	7	8	9
11	6	7	8	9	10	5	0	1	2	3	4
10	11	6	7	8	9	4	5	0	1	2	3
6	7	8	9	10	11	0	1	2	3	4	5
9	10	11	6	7	8	3	4	5	0	1	2
5	0	1	2	3	4	11	6	7	8	9	10
3	4	5	0	1	2	9	10	11	6	7	8
1	2	3	4	5	0	7	8	9	10	11	6

VI. Projecting Diagonals Construction of O(n, t) Sets

A very simple procedure (sort of the "man-on-the-street" approach) of constructing balanced incomplete block and partially balanced incomplete block designs for $v = k^2$ items in incomplete blocks of size k has been utilized since the late 1940's by the author and has its counterpart in constructing O(n,t) sets. First we shall illustrate its use in incomplete block experiment design construction, and then we show how it applies to the construction on O(n,t) set. The theoretical basis for this method may be derived directly from the preceding section.

The procedure becomes apparent through an example. Suppose that $v = 9$ and $k = 3$. After writing the first square as illustrated below, take successive diagonals of the preceding square and use them to form the incomplete blocks of a square, thus:

Square 1

1	2	3
4	5	6
7	8	9

Square 2

1	5	9
2	6	7
3	4	8

Square 3

1	6	8
2	4	9
3	5	7

Square 4

1	4	7
2	5	8
3	6	9

As we have noted this is a resolvable balanced incomplete design with the parameters $v = 9 = k^2$, $k = 3$, $r = 4 = k + 1$, $b = 12 = k(k+1)$, and $\lambda = 1$, where the rows of the above squares form the incomplete blocks.

To form a partially balanced incomplete block design for $v = k^2$ in incomplete blocks of size k one may use any 2, any 3, ..., any k arrangements (or squares). To illustrate the formation of a partially balanced incomplete block

design for $v = 6 = k(k-1)$, $r = 2, 3, \ldots, k$, and $k' = k-1 = 2$ simply delete the last set of k numbers, i.e. 7, 8, and 9 from the last $k = 3$ arrangements. The deletion of certain symbols from the set $1, 2, \ldots, v$ is known as "variety cutting". For $k^2 = 25$ and $k = 5$ partially balanced incomplete block designs may be constructed for $v = 10$ and $k^* = 2$, $v = 15$ and $k^+ = 3$, and $v = 20$ and $k' = 4$ by the above "variety cutting" procedure.

Also, the successive diagonals method is useful for $v = k^2$ in incomplete blocks of size k for any odd k. For example, for $v = 225$ and $k = 15$ four arrangements or squares may be quickly constructed by the above method. Likewise, the "variety cutting" procedure may be utilized to obtain 2 or 3 arrangements for $v = 15p$, $2 \leq p \leq 15$, varieties in incomplete blocks of size p.

The above method has its counterpart in constructing mutually orthogonal latin squares and this possibility is briefly mentioned in Fisher and Yates [1957] in this context. Again the method becomes apparent through an example. First write the latin square in standard order and of the form given below for the first square, then project the main right diagonal of the preceding square into the first column of a square, and then write the symbol order in the same manner as in the first square. As a first example, let the order of the latin square be 3; the squares are:

first square

1	2	3
2	3	1
3	1	2

second square

1	2	3
3	1	2
2	3	1

third square

1	2	3
1	2	3
1	2	3

Thus, the main right diagonal of the first square is 1,3,2 which becomes the first column of the second square. Then, write the first row as 1,2,3, the second row as 3,1,2, and the third row as 2,3,1. For the third square, which is not a latin square, the right main diagonal of the second square is 1,1,1 and this becomes the first column of the third square; the rows are then completed. If we then take the right main diagonal of the third square, we obtain the first square.

As a second illustrative example, the five squares for order $n = 5$ which are constructed by successively projecting diagonals, are:

first square

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

second square

1	2	3	4	5
3	4	5	1	2
5	1	2	3	4
2	3	4	5	1
4	5	1	2	3

third square

1	2	3	4	5
4	5	1	2	3
2	3	4	5	1
5	1	2	3	4
3	4	5	1	2

fourth square

1	2	3	4	5
5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1

fifth square

1	2	3	4	5
1	2	3	4	5
1	2	3	4	5
1	2	3	4	5
1	2	3	4	5

The fifth square is not a latin square but may be utilized to construct the first square through use of the method of successive projections of the main diagonals.

The method may be utilized for any odd order n and will produce $q_1 - 1$ orthogonal latin squares for $n = q_1\, q_2 \ldots q_s$ where $q_i < q_{i+1}$ and $q_1\, q_2 \ldots q_s$

is the prime power decomposition of n. Thus, for $n = 15 = 3(5)$ a pair $(q_1 - 1 = 3 - 1 = 2)$ of orthogonal latin squares is easily produced. For $n = 35 = 5(7)$, a quartet of mutually orthogonal latin squares is readily produced by the projecting diagonals method.

VII. Relations Between Complete Confounding and Simple Orthomorphisms

We shall illustrate the ideas by going through a complete example taking $n = 12 = 2^2 \times 3$. For this purpose we take the ring of 12 elements (obtained by utilizing Raktoe's [1969] results) as follows:

$GF(2^2)$		I_3	$GF(3)$		I_4
0		0	0		0
1	$\Rightarrow$	3	1	$\Rightarrow$	4
x		3x	2		2
x+1		3x+3			

$R_{12} = I_3 \oplus I_4 = \{0, 1, 2, 3, 4, 5, 3x, 3x+1, 3x+2, 3x+3, 3x+4, 3x+5\}$

R_{12} is a commutative ring under addition and multiplication (mod (6, $3x^2 + 3x + 3$) in the following sense:

e.g.: (a). $(3x+3) + (3x+4) = 6x + 7 = 1$; here we have to reduce only mod 6 to get the answer.

(b). $(3x+1) \cdot (3x+4) = 9x^2 + 15x + 4$

$\equiv 3x^2 + 3x + 4 \equiv 1$.

Explicitly, to facilitate arithmetic, the addition and mutliplication of these 12 elements are:

+	0	1	2	3	4	5	3x	3x+1	3x+2	3x+3	3x+4	3x+5
0	0	1	2	3	4	5	3x	3x+1	3x+2	3x+3	3x+4	3x+5
1		2	3	4	5	0	3x+1	3x+2	3x+3	3x+4	3x+5	3x
2			4	5	0	1	3x+2	3x+3	3x+4	3x+5	3x	3x+1
3				0	1	2	3x+3	3x+4	3x+5	3x	3x+1	3x+2
4					2	3	3x+4	3x+5	3x	3x+1	3x+2	3x+3
5						4	3x+5	3x	3x+1	3x+2	3x+3	3x+4
3x							0	1	2	3	4	5
3x+1								2	3	4	5	0
3x+2									4	5	0	1
3x+3										0	1	2
3x+4											2	3
3x+5												4

•	0	1	2	3	4	5	3x	3x+1	3x+2	3x+3	3x+4	3x+5
0	0	0	0	0	0	0	0	0	0	0	0	0
1		1	2	3	4	5	3x	3x+1	3x+2	3x+3	3x+4	3x+5
2			4	0	2	4	0	2	4	0	2	4
3				3	0	3	3x	3x+3	3x	3x+3	3x	3x+3
4					4	2	0	4	2	0	4	2
5						1	3x	3x+5	3x+4	3x+3	3x+2	3x+1
3x							3x+3	3	3x+3	3	3x+3	3
3x+1								3x+4	5	3x	1	3x+2
3x+2									3x+1	3	3x+5	1
3x+3										3x+3	3	3x
3x+4											3x+1	5
3x+5												3x+4

Now, associate with a latin square of order 12 the $3^2 \times 4^2 = [3 \times 4] \times [3 \times 4]$ $= 12 \times 12$ lattice square with the following breakdown of the 143 degrees of freedom corresponding to a four-factor factorial:

A^4	2	C^3	3
B^4	2	D^3	3
A^4B^4	2	C^3D^3	3
A^4B^2	2	C^3D^{3x}	3
		C^3D^{3x+3}	3

A^4C^3	6	B^4C^3	6	$A^4B^4C^3$	6	$A^4B^2C^3$	6
A^4D^3	6	B^4D^3	6	$A^4B^4D^3$	6	$A^4B^2D^3$	6
$A^4C^3D^3$	6	$B^4C^3D^3$	6	$A^4B^4C^3D^3$	6	$A^4B^2C^3D^3$	6
$A^4C^3D^{3x}$	6	$B^4C^3D^{3x}$	6	$A^4B^4C^3D^{3x}$	6	$A^4B^2C^3D^{3x}$	6
$A^4C^3D^{3x+3}$	6	$B^4C^3D^{3x+3}$	6	$A^4B^4C^3D^{3x+3}$	6	$A^4B^2C^3D^{3x+3}$	6

For any row or column confounding we need to confound effects totaling up to 11 degrees of freedom. There are natural candidates available. In fact, we may choose for our first lattice square the confounding scheme in many ways. A scheme resulting in a pair of orthogonal latin squares is the following:

Confounding scheme of our 12 × 12 lattice square

	$(A^4C^3)_0$	$(A^4C^3)_1$	$(A^4C^3)_2$	$(A^4C^3)_3$	$(A^4C^3)_4$	$(A^4C^3)_5$	$(A^4C^3)_{3x}$	$(A^4C^3)_{3x+1}$	$(A^4C^3)_{3x+2}$	$(A^4C^3)_{3x+3}$	$(A^4C^3)_{3x+4}$	$(A^4C^3)_{3x+5}$
$(B^4D^3)_0$	0000	4030	2000	0030	4000	2030	00 3x 0	40 3x+3 0	20 3x 0	00 3x+3 0	40 3x 0	20 3x+3 0
$(B^4D^3)_1$	0403	4433	2403	0433	4403	2433	04 3x 3	44 3x+3 3	24 3x 3	04 3x+3 3	44 3x 3	24 3x+3 3
$(B^4D^3)_2$	0200	4230	2200	0230	4200	2230	02 3x 0	42 3x+3 0	22 3x 0	02 3x+3 0	42 3x 0	22 3x+3 0
$(B^4D^3)_3$	0003	4033	2003	0033	4003	2033	00 3x 3	40 3x+3 3	20 3x 3	00 3x+3 3	40 3x 3	20 3x+3 3
$(B^4D^3)_4$	0400	4430	2400	0430	4400	2430	04 3x 0	44 3x+3 0	24 3x 0	04 3x+3 0	44 3x 0	24 3x+3 0
$(B^4D^3)_5$	0203	4233	2203	0233	4203	2233	02 3x 3	42 3x+3 3	22 3x 3	02 3x+3 3	42 3x 3	22 3x+3 3
$(B^4D^3)_{3x}$	000 3x	403 3x	200 3x	003 3x	400 3x	203 3x	00 3x 3x	40 3x+3 3x	20 3x 3x	00 3x+3 3x	40 3x 3x	20 3x+3 3x
$(B^4D^3)_{3x+1}$	040 3x+3	443 3x+3	240 3x+3	043 3x+3	440 3x+3	243 3x+3	04 3x 3x+3	44 3x+3 3x+3	24 3x 3x+3	04 3x+3 3x+3	44 3x 3x+3	24 3x+3 3x+3
$(B^4D^3)_{3x+2}$	020 3x	423 3x	220 3x	023 3x	420 3x	223 3x	02 3x 3x	42 3x+3 3x	22 3x 3x	02 3x+3 3x	42 3x 3x	22 3x+3 3x
$(B^4D^3)_{3x+3}$	000 3x+3	403 3x+3	200 3x+3	003 3x+3	400 3x+3	203 3x+3	00 3x 3x+3	40 3x+3 3x+3	20 3x 3x+3	00 3x+3 3x+3	40 3x 3x+3	20 3x+3 3x+3
$(B^4D^3)_{3x+4}$	040 3x	443 3x	240 3x	043 3x	440 3x	243 3x	04 3x 3x	44 3x+3 3x	24 3x 3x	04 3x+3 3x	44 3x 3x	24 3x+3 3x
$(B^4D^3)_{3x+5}$	020 3x+3	423 3x+3	220 3x+3	023 3x+3	420 3x+3	223 3x+3	02 3x 3x+3	42 3x+3 3x+3	22 3x 3x+3	02 3x+3 3x+3	42 3x 3x+3	22 3x+3 3x+3

LATIN SQUARE 1: Treatments identified with $A^4 B^4 C^3 D^3$

0	1	2	3	4	5	3x	3x+1	3x+2	3x+3	3x+4	3x+5
1	2	3	4	5	0	3x+1	3x+2	3x+3	3x+4	3x+5	3x
2	3	4	5	0	1	3x+2	3x+3	3x+4	3x+5	3x	3x+1
3	4	5	0	1	2	3x+3	3x+4	3x+5	3x	3x+1	3x+2
4	5	0	1	2	3	3x+4	3x+5	3x	3x+1	3x+2	3x+3
5	0	1	2	3	4	3x+5	3x	3x+1	3x+2	3x+3	3x+4
3x	3x+1	3x+2	3x+3	3x+4	3x+5	0	1	2	3	4	5
3x+1	3x+2	3x+3	3x+4	3x+5	3x	1	2	3	4	5	0
3x+2	3x+3	3x+4	3x+5	3x	3x+1	2	3	4	5	0	1
3x+3	3x+4	3x+5	3x	3x+1	3x+2	3	4	5	0	1	2
3x+4	3x+5	3x	3x+1	3x+2	3x+3	4	5	0	1	2	3
3x+5	3x	3x+1	3x+2	3x+3	3x+4	5	0	1	2	3	4

LATIN SQUARE 2: Treatments identified with $A^4B^2C^3D^{3x}$

0	1	2	3	4	5	3x	3x+1	3x+2	3x+3	3x+4	3x+5
3x+2	3x+3	3x+4	3x+5	3x	3x+1	2	3	4	5	0	1
4	5	0	1	2	3	3x+4	3x+5	3x	3x+1	3x+2	3x+3
3x	3x+1	3x+2	3x+3	3x+4	3x+5	0	1	2	3	4	5
2	3	4	5	0	1	3x+2	3x+3	3x+4	3x+5	3x	3x+1
3x+4	3x+5	3x	3x+1	3x+2	3x+3	4	5	0	1	2	3
3x+3	3x+4	3x+5	3x	3x+1	3x+2	3	4	5	0	1	2
5	0	1	2	3	4	3x+5	3x	3x+1	3x+2	3x+3	3x+4
3x+1	3x+2	3x+3	3x+4	3x+5	3x	1	2	3	4	5	0
3	4	5	0	1	2	3x+3	3x+4	3x+5	3x	3x+1	3x+2
3x+5	3x	3x+1	3x+2	3x+3	3x+4	5	0	1	2	3	4
1	2	3	4	5	0	3x+1	3x+2	3x+3	3x+4	3x+5	3x

Using the complete confounding approach as outlined above, one can construct min $[(2^2-1), (3-1)] = 2$ mutually orthogonal latin squares and no more as can easily be observed from the degrees of freedom table.

From the multiplication table of our ring R_{12}, we observe that 1, 5, 3x+1, 3x+2, 3x+4 and 3x+5 are the 6 non-zero divisors (i.e. elements with multiplicative inverses). Following Bose, Chakravarti and Knuth [1960], we consider simple automorphisms in R_{12} of the form:

$$\alpha(r) = r^* r$$

where r^* is a given fixed element having a multiplicative inverse (because only these elements are capable of producing automorphisms of R_{12}). Let now our aim be to produce two orthomorphisms which in turn will produce an O(12, 2) set. For this purpose consider the automorphisms:

$$I(r) = r$$

$$\alpha(r) = r^* \cdot r \quad .$$

Now I is orthogonal to α which implies the condition that r in the equation $[r^* \cdot r - r] = c$ has a unique solution for every c of R_{12} (see Mann [1949], pp. 103-105). In our setting this means that $r(r^* - 1) = c$ has a unique solution, i.e., $r(r^* + 5) = c$ has a unique solution which in turn implies that $(r^* + 5)^{-1}$ exists in R_{12}.

Substituting in the values of r^* we see that:

$[1 + 5]^{-1}$ does not exist in R_{12}

$[5 + 5]^{-1}$ " " " " "

$[(3x+1] + 5]^{-1}$ does not exist in R_{12}

$$[(3x+2)+5]^{-1} = [3x+1]^{-1} \text{ exists in } R_{12}$$

$$[(3x+4)+5]^{-1} \text{ does not exist in } R_{12}$$

$$[(3x+5)+5]^{-1} = [3x+4]^{-1} \text{ exists in } R_{12} .$$

Hence we have obtained two pairs of orthomorphisms namely:

$$I(r) = r \qquad I(r) = r$$

and

$$\alpha_1(r) = (3x+2)r \qquad \alpha_2(r) = (3x+5)r .$$

The O(12, 2) set presented above using complete confounding corresponds to the first pair of maps. It may be easily shown that simple maps of the type $\alpha(r) = r^* \cdot r$ lead to O(12, 2) sets or in general to an O(n, a) set, where $a = \min (p_1^{n_1} - 1, p_2^{n_2} - 1, \ldots, p_k^{n_k} - 1)$ and $n = \prod_{i=1}^{k} p_i^{n_i}$ so that the complete confounding approach is equivalent to the construction of a set of a orthomorphisms.

VIII. Some Remarks on "Orthomorphism" Construction of O(n, t) Sets

In 1959 and/or 1960 E. T. Parker showed by a combination of classification of cases (with considerable elimination of isomorphic repetition accessible to cut down on computer time, followed by computer runs) that there are obtainable only 5 orthogonal latin squares of order 12, all restricted to be copies of the non-cyclic Abelian group with latin squares related by row permutations. (Some researchers [6, 31] call this the method of orthomorphisms. Parker considers this no method, but only based on freaks of luck; further, Parker feels that "orthomorphism" admits no precise definition.)

Parker made another finding, also by hard classification of cases followed by computer runs, which Marshall Hall feels is more important than that cited above. No pair of order-12 orthogonal squares of the type mentioned can be extended to a complete set of any sort; i.e., further orthogonal latin squares are allowed to be completely general.

What might be obtainable for orthogonal squares of order 20 in like fashion, row-permuting the non-cyclic Abelian group of order 20, is an interesting matter for speculation — conceivably one might even produce a complete set (19 orthogonal squares equivalent to a plane). Knuth and Parker discussed the problem about 1963, and concluded that exhaustive search is out of the question; still a fortunate sample of cases might produce an attractive result.

In 1960 Parker looked at the row-permutation ("orthomorphism" of Bose and Mendelsohn) approach for the group of order 15, and proved by Hasse-Minkowski invariants that a complete set could not be so obtained. He dropped

further work; but some persistence could quite possibly yield as much as five orthogonal squares of order 15 .

A hybrid attack on order 15 or 20 might be undertaken by an ambitious investigator. (The facts for order 12 mentioned above rule out chances here.) One might produce sets of orthogonal latin squares of row-permuted group type, using automorphisms of the group latin squares to eliminate — or, that failing, reduce — isomorphic repetition. It would not be shrewd to program a computer to produce all transversals of a group latin square, for running time and output would be excessive; then for any hint of efficiency it would be necessary to turn about and do a reduction on the computer output. After a set of row-permuted latin squares (possibly exhaustive for order 15, but almost certainly only a sample for order 20) large enough that computer searching would require realistic amounts of time, one might proceed with the next step. Produce all transversals of the set of orthogonal squares by computer, then fit these together in all possible ways (again by computer) to form orthogonal mates of the preceding set of orthogonal latin squares. Unlike Parker's assertion above about complete sets of order-15 squares, there is no known argument implying impossibility of producing 14 orthogonal latin squares of order 15 by this hybrid attack.

IX. Oval Construction of O(n, t) Sets

The approach to construction of finite projective planes used here differs from the ones known in the literature. The main idea is to make use of the maximum number of points no three on one line in a finite projective plane of even order called henceforth an oval. The oval cannot consist of more than $n+2$ points in a plane of order n. This is obvious since through each point pass $n+1$ lines and the lines through any point of the oval can contain at most one more point of the oval. On the other hand, if a plane of order n does include an oval consisting of the maximum number of points, namely $n+2$, then the lines of the plane can be classified into two categories in respect to this oval. One category consists of lines intersecting the oval in two points called secants, the other of lines having no points of the oval called non-intersectors. The number of secants is clearly $\frac{(n+2)(n+1)}{2}$ and the number of non-intersectors is $\frac{n(n-1)}{2}$. Through each of the n^2-1 points which do not belong to the oval there would have to pass $\frac{n+2}{2}$ secants and $\frac{n}{2}$ non-intersectors. Hence, n must be even.

It is well-known that removing one line from the plane, usually called the line at infinity, the remaining $n^2 + n$ lines can be arranged into $2n$ lines passing through two points at infinity which are arbitrary up to notation and coordinatization of the plane, and n^2-n lines belonging to $n-1$ mutually orthogonal latin squares. If the line at infinity is chosen to be a secant and there are $2n$ lines, the lines pass through the two points of the oval such that each of the $n-1$ latin squares consists of $\frac{n}{2}$ secants and $\frac{n}{2}$ non-intersectors passing through each of the $n-1$ points at infinity other than the points of the oval. The $2n$ lines correspond to the rows and columns of the latin square.

Using the described method, it was assumed that a plane of order 10 exists. Under this assumption 21 lines could be exhibited arbitrarily up to notation. Out of these lines one was taken to be the line at infinity and the remaining 20 used to coordinatize the plane. Then by trial and error twenty more lines were found which formed two orthogonal latin squares. The method used to construct these squares differs from the one described in the literature.

Unfortunately no more squares could be found using this method and a high speed computer established that the two squares did not yield an additional mutually orthogonal mate. Clearly it could happen that the choice of the first two was unfortunate. The same method was applied to the plane of order 12 . Here the trial and error method failed to produce even two orthogonal squares. It may be worthwhile to remark that the construction of the plane and consequently the search for orthogonal latin squares does not require the assumption that the oval consists of the maximum number of points $n + 2$. However, if the plane does not include an oval consisting of $n + 2$ points the lines could not be classified into two categories only and this complicates the construction of the plane. Let us illustrate the method in the case n equals 10 . It is easy to show that in this case the oval must consist of at least 6 points. However, the case of an oval of 6 points would be ignored since in this case every quadrangle would have to have collinear diagonals. On the other hand, a plane of order ten must be non-Desarguessian and hence must contain

a nondegenerate quadrangle with noncollinear diagonals. Suppose that the plane contains a quadrangle with noncollinear diagonals and suppose that the plane contains an oval consisting of seven points then the 104 points of the plane which do not belong to the oval could be classified into three categories:

(i) points lying on 3 secants, 1 tangent 7 nonintersectors

(ii) " " " 2 " 3 " 6 "

(iii) " " " 1 " 5 " 5 "

Let us name the number of points in each category by x, y, z respectively. Clearly $x + y + z = 104$.

Counting the intersections of the secants and the tangents we get the further equations:

$$3x + y = 105$$

$$3y + 10z = 525$$

The unique solutions of this system of equations are $x = 20$, $y = 45$, $z = 39$. One could start the construction of the plane under the present assumption and investigate the possibilities of obtaining orthogonal latin squares in this way.

X. Code Construction of O(n, t) Sets

Given an n-symbol alphabet, e.g., $1,2,\ldots,n$, and a set of k-tuples of the n symbols, we denote the set of all k-tuples by $C_{k,n}$. This set may be thought of as a vector space or as a k-dimensional hypercube with edges of length n. Any subset of $C_{k,n}$ is denoted as a block code with a block length of k. The elements of the subset are denoted as code words. The number of symbols by which any two code words differ is called the Hamming distance. If any pair of code words in the subset differs by a Hamming distance of at least r, the block code is called a distance r code. A distance r code is called an $(r-1)/2$-error correcting code because fewer than $(r-1)/2$ changes leaves the word closer to its original form than to any other code word in the subset. For similar reasons, a distance r code has also been designated as an $(r-1)$-error-dectecting code.

In an interesting paper, Golomb and Posner [1964] discuss the relationships between a subset of n^2 code words and an O(n,t) set and relate these to ideas developed from a consideration of a set of n^2 super rooks of power t on an n^{t+2} chessboard such that no two super rooks attack each other. The new concepts of rook domains and rook packing were found to be very useful in providing a geometrical view of the results.

Any subset of n^2 words from $C_{3,n}$ which forms a single-error-detecting code may be used to construct a latin square of order n as any pair of the triples differs by at least two symbols. Likewise, any subset of n^2 words

from $C_{t+2,n}$ with a Hamming distance of $t+1$ may be utilized to construct an $O(n,t)$ set. These results are embodied in the following theorem (from Golomb and Posner [1964]):

Theorem X.1. The following three concepts are equivalent:

i) an $O(n,t)$ set.

ii) A set of n^2 nonattacking super rooks of power t on the n^{t+2} board. For even t, also the following, a set of n^2 super rooks of power $t/2$ on the n^{t+2} board such that no cell is attacked twice; that is, such that the rook domains are nonoverlapping.

iii) A distance $t+1$ code of block length $t+2$ with n^2 words from an n-symbol alphabet.

For those interested in code construction, reference may be made to Mann [1968] and Peterson [1961] and the literature citations therein. We shall merely illustrate the method of construction of an $O(n,t)$ set from n^2 words of length $t+2$ and Hamming distance $t+1$ through an example. Let $n = 3$ and $t = 2$. Then the $n^2 = 9$ code words with length 4 and Hamming distance 3 and the corresponding latin squares are:

				latin squares of order 3								
					0	1	2			0	1	2
0000	0111	0222		0	0	1	2		0	0	1	2
1012	1120	1201	to produce	1	1	2	0	and	1	2	0	1
2021	2102	2210		2	2	0	1		2	1	2	0

where the first symbol corresponds to row number, the second to column number,

the third to symbols in the first latin square, and the fourth to symbols in the second latin square. The two latin squares form an $O(3,2)$ set. Note that any pair of the quadruples differs in at least three symbols.

The analogy of the above with many of the concepts from fractional replication and orthogonal arrays is immediately apparent. The equivalences of many of the results in these fields need to be systematically noted much in the same manner that Golomb and Posner [1964] note various equivalences among $O(n,t)$ sets, error-correcting codes, and n^2 nonattacking rooks on an n^{t+2} chessboard.

XI. Pairwise Balanced Design Construction of O(n, t) Sets

Central to the constructions of orthogonal latin squares of Bose and Shrikhande [1959] and of Parker [1959, 1960] is the following which might be called a "Folk theorem," being credited to no specific investigator: From a set of t orthogonal latin squares of order n one may produce a set of n^2 ordered (t+2)-tuples on n symbols such that each pair of distinct positions contains each ordered pair of symbols (exactly once); the converse construction can also be carried out. (Some, such as Bose, prefer to call the set of (t+2)-tuples an orthogonal array.) There is nothing difficult to prove in this construction. Two arbitrary positions in the (t+2)-tuples are identified with row and column indices in matrices, and each other position with entries in one of the matrices. The equivalence between orthogonality of latin squares and the conditions on the (t+2)-tuples is then fairly apparent.

Parker [1960] contributed the following to the construction of orthogonal latin squares. If there exists a pair of orthogonal latin squares of order m, then there exists a pair of orthogonal latin squares of order $3m + 1$.

Let the $3m + 1$ symbols be $X_1, \ldots, X_m$ and the residue classes (mod $2m + 1$). Form the (latin square) array

$$A: \begin{matrix} X_i & 0 & i & -i \\ 0 & X_i & -i & i \\ i & -i & X_i & 0 \\ -i & i & 0 & X_i \end{matrix} .$$

For each i, $1 \leq i \leq m$, each row of A an ordered quadruple. In turn, the list of quadruples is built up by adding each integer (mod $2m + 1$) to all four positions at once, the X_i symbols being unchanged by the addition. The set of $4m(2m + 1)$ ordered quadruples just described contains in each pair of distinct positions exactly one occurrence of each ordered pair made up of an X_i and a residue class in either order, and of each ordered pair made up of two distinct residue classes. The required set of ordered quadruples is completed by adjoining: i) all ordered quadruples (j,j,j,j), $j = 0, \ldots, 2m$; ii) a set of ordered quadruples on the X_i symbols corresponding to a pair of orthogonal latin squares of order m guaranteed by the hypothesis to exist.

Bose and Shrikhande (1959, published 1959 and 1960 partly in a 3-author paper with Parker) developed a sequence of constructive theorems which led in steps to disproof of Euler's conjecture for all orders $4t + 2 > 6$. Their central theorem given here does not exhaust their methods, but virtually all their results rest on this theorem. We begin with a definition. A pairwise balanced design, $PB(n; k_1,\ldots,k_t)$ is a collection of subsets of a set of n elements, each subset having number of elements one of the k_i, and such that each pair of distinct elements in the set of n occurs in a unique subset of the PB. (Note: unlike in balanced incomplete block designs, the subsets of a PB are not restricted to have equal numbers of elements.) Now for the main theorem of Bose and Shrikhande. If a $PB(n; k_1,\ldots,k_t)$ exists, and for each i, $1 \leq i \leq t$, a set of m orthogonal latin squares of order k_i exists, then a set of $m-1$ orthogonal latin squares of order n exists. Loosely speaking, the sets of ordered tuples for each subset

of the PB are constructed and these fit together to form a set of ordered tuples for the full set of n elements. The decrease from m to m-1 orthogonal latin squares occurs because in fitting the pieces together to form the large set of ordered tuples, it is necessary that each set of ordered tuples formed from a subset of the PB include each (i,i,...,i), where i ranges over the elements of that subset. (It is sufficient that this condition be fulfilled in the construction. Thus the theorem might be stated in slightly stronger form: "If ... $1 \leq i \leq t$, a set of m orthogonal latin squares of order k_i with a transversal exists, then a set of m orthogonal latin squares of order n exists.") Now for a more nearly formal version of the proof. If there exists a set of m orthogonal latin squares of order n, then there exists a set of the appropriate sort of n^2 ordered (m+1)-tuples with each symbol repeated in an (m+1)-tuple m+1 times. (The condition mentioned is satisfied with (m+2)-tuples if the set of orthogonal latin squares has a transversal.) One need simply put together the ordered tuples on each subset of the PB in turn, subject to the important condition that within each subset of the PB, each tuple of repetitions of each symbol be included. Carrying this out on the alphabet of the symbols in each subset of the PB, one has the construction for the set of orthogonal latin squares in the conclusion; each ordered tuple of a repeated symbol among the n is used only once.

A representative and very interesting example (Bose and Shrikhande informed Parker that this was the first case of disproof of Euler's conjecture produced in their joint work at a blackboard) yields 5 mutually orthogonal latin squares of order 50 via the PB construction. One forms the affine plane of

order 7, then adjoins exactly one ideal point on each line of one class of parallel lines. This yields a PB(50; 8,7). Since there exist 6 orthogonal latin squares of each order 8 and 7, there exist 6 - 1 = 5 orthogonal latin squares of order 50 .

There is a limitation on the Bose-Shrikhande PB construction. Aside from trivial PB designs, having a single subset of all elements, any PB has a subset with at most one more element than the square root of the number of elements in the large set. Thus other techniques are requisite to produce more than $\sqrt{n}$ orthogonal latin squares of order not a prime-power.

XII. Product Composition of O(n, t) Sets

About 70 years ago, for the first time, Tarry [1899] in his half-page note asserted that if there exists an O(a, 2) set and if there exists an O(b, 2) set then there exists an O(ab, 2) set. He exhibited the following O(12, 2) set, by composing two O(3, 2) and O(4, 2) sets, to demonstrate the truth of his assertion. Note that in the following square the set of first integers belong to one latin square and the set of second integers belong to the second latin square. No more description is given by Tarry.

2-3	1-1	3-2	8-12	7-10	4-11	11-6	10-4	12-5	5-9	4-7	6-8
3-1	2-2	1-3	9-10	8-11	7-12	12-4	11-5	10-6	6-7	5-8	4-9
1-2	3-3	2-1	7-11	0-12	8-10	10-5	12-6	11-4	4-8	6-9	5-7
11-9	10-7	12-8	5-6	4-4	6-5	2-12	1-10	3-11	8-3	7-1	9-2
12-7	11-8	10-9	6-4	5-5	4-6	3-10	2-11	1-12	9-1	8-2	7-3
10-8	12-9	11-7	4-5	6-6	5-4	1-11	3-12	2-10	7-2	9-3	8-1
5-12	4-10	6-11	11-3	10-1	12-2	8-9	7-7	9-8	2-6	1-4	3-5
6-10	5-11	4-12	12-1	11-2	10-3	9-7	8-8	7-9	3-4	2-5	1-6
4-11	6-12	5-10	10-2	12-3	11-1	7-8	9-9	8-7	1-5	3-6	2-4
8-6	7-4	9-5	2-9	1-7	3-8	5-3	4-1	6-2	11-12	10-10	12-11
9-4	8-5	7-6	3-7	2-8	1-9	6-1	5-2	4-3	12-10	11-11	10-12
7-5	9-6	8-4	1-8	3-9	2-7	4-2	6-3	5-1	10-11	12-12	11-10

Tarry did not observe any generalization of his method. Perhaps this was due to the fact that he, like so many other researchers, was only concerned with sets of type O(n, 2) . Probably he was not aware of the existence of a larger set.

About 23 years later MacNeish [1922] demonstrated:

1) The existence and a construction of an $O(n, n-1)$ set for n a prime or prime power integer.

2) A generalization of Tarry's procedure *viz.*, if there exists an $O(a, r)$ set and if there exists an $O(b, r)$ set then there exists an $O(ab, r)$ set.

3) By a successive application of 1) and 2) he showed that if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ is the prime-power decomposition of n then there exists an $O(n, r)$ set where $r = \min\{p_i^{\alpha_i} - 1,\ i = 1, 2, \ldots, t\}$.

MacNeish could not embed his $O(n, r)$ set generated in 3) in a larger set. This unsuccessful attempt, reinforced by Euler's conjecture, led MacNeish to prove (erroneously) geometrically that $O(n,z)$ sets do not exist for $z > r$, and therefore, as a confirmation of Euler's conjecture. The preceding argument of MacNeish is known as MacNeish's conjecture in the literature. By constructing an $O(21, 3)$ set Parker [1959] gave a counter example to MacNeish's conjecture. Later Bose, Shrikhande, and Parker [1960] completely demolished Euler's conjecture except for $n = 6$. It should be mentioned that MacNeish's conjecture has not been totally disproved yet. For instance, no one as yet as far as we know, has constructed an $O(15, 4)$ set (an $O(15, 3)$ set is given in section V for the first time) or an $O(20, 3)$ set. We believe that MacNeish should be given substantial credit for his non-erroneous contributions. It is to be regretted that MacNeish is often cited in the literature only for his false conjecture.

Even though Tarry and MacNeish did not attach any name to their procedure, it is not difficult to see that it is the method of Kronecker product of matrices. Therefore, we can state, more formally, their results as follows:

Theorem (Tarry-MacNeish). If $\{A_1, A_2, \ldots, A_r\}$ is an $O(n,r)$ set and if $\{B_1, B_2, \ldots, B_r\}$ is an $O(m,r)$ set, then $\{A_1 \otimes B_1, A_2 \otimes B_2, \ldots, A_r \otimes B_r\}$, where $\otimes$ denotes the Kronecker product operation of matrices, is an $O(nm, r)$ set.

The preceding arguments clearly support the choice of the title for this section and is in contrast to the choice of the name for the procedure given in section XIII.

XIII. Sum Composition Construction of O(n, t) Sets

XIII.1. Introduction

Perhaps one of the most useful techniques for the construction of combinatorial systems is the method of composition. To mention some, here are few well-known examples: 1) If there exists a set of t orthogonal latin squares of order n_1 and if there exists a set of t orthogonal latin squares of order n_2, then there exists a set of t orthogonal latin squares of order n_1n_2. 2) If there are Steiner triple systems of order v_1 and v_2, there is a Steiner triple system of order $v = v_1v_2$. 3) If H_1 and H_2 are two Hadamard matrices of order n_1 and n_2 respectively, then the Kronecker product of H_1 and H_2 is a Hadamard matrix of order n_1n_2. 4) If Room squares of order n_1 and n_2 exist, then a Room square of order n_1n_2 exists. 5) If BIB (v, k, λ_1) and BIB (v_2, k, λ_2) exist and if $f(\lambda_2 v_2^2) \geq k$, then BIB $(v_1v_2, k, \lambda_1\lambda_2)$ exists where $f(\lambda_2 v_2^2)$ denotes the maximum number of constraints which are possible in an orthogonal array of size $\lambda_2 v_2^2$, with v_2 levels, strength 2, and index λ_2. 6) As a final example, the existence of orthogonal arrays $(\lambda_i v_i^t, q_i, v_i, t)$, $i = 1, 2, \ldots, r$ implies the existence of the orthogonal array $(\lambda v^t, q, v, t)$, where $\lambda = \lambda_1\lambda_2\ldots\lambda_r$, $v = v_1v_2\ldots v_r$, and $q = \min(q_1, q_2, \ldots, q_r)$.

The reader will note that each of the above examples involved a product type composition. The method that we will describe utilizes a sum type composition, by means of which one can possibly construct sets of orthogonal latin squares for all $n \geq 10$.

XIII.2. Definitions

In the sequel by an $O(n, t)$ set we mean a set of t mutually orthogonal latin squares of order n.

a) A transversal (directrix) of a latin square L of order n on an n-set Σ is a collection of n cells such that the entries of these cells exhaust the set Σ and every row and column of L is represented in this collection. Two transversals are said to be parallel if they have no cell in common.

b) A collection of n cells is said to form a common transversal for an $O(n, t)$ set if the collection is a transversal for each of these t latin squares. Two common transversals are said to be parallel if they have no cell in common.

Example. The underlined and parenthesized cells form two parallel common transversals for the following $O(4, 2)$ set.

$$\left\{\begin{array}{cccc} 1 & 2 & (3) & \underline{4} \\ (2) & \underline{1} & 4 & 3 \\ \underline{3} & (4) & 1 & 2 \\ 4 & 3 & \underline{2} & (1) \end{array}\right. \qquad \left.\begin{array}{cccc} 1 & 2 & (3) & \underline{4} \\ (4) & \underline{3} & 2 & 1 \\ \underline{2} & (1) & 4 & 3 \\ 3 & 4 & \underline{1} & (2) \end{array}\right\}$$

XIII.3. Composing Two Latin Squares of Order n_1 and n_2

A very natural question in the theory of latin squares is the following: Given two latin squares L_1 and L_2 of order n_1 and n_2 $(n_1 \geq n_2)$ respectively. In how many ways can one compose L_1 and L_2 in order to obtain a latin square L_3 of order m, where m is a function of n_1 and n_2 only? This question can be partially answered as follows. First, it is well-known that the Kronecker product $L_3 = L_1 \otimes L_2$ is a latin square of order $m = n_1 n_2$ irrespective of the combinatorial structure of L_1 and L_2. Secondly, we show that if L_1 has a certain combinatorial structure, then one can construct a latin square L of

order $n = n_1 + n_2$. Naturally enough we call this procedure a "method of sum composition".

Even though our method of sum composition does not work for all pairs of latin squares, it has an immediate application in the construction of orthogonal latin squares including those of order $4t + 2$, $t \geq 2$. We emphasize that the combinatorial structure of orthogonal latin squares constructed by the method of sum composition is completely different from those of known orthogonal latin squares in the literature. Therefore, it is worthwhile to study these squares for the purpose of constructing new finite projective planes.

We shall now describe the method of "sum composition". Let L_1 and L_2 be two latin squares of order n_1 and n_2, $n_1 \geq n_2$, on two non-intersecting sets $\Sigma_1 = \{a_1, a_2, \ldots, a_{n_1}\}$ and $\Sigma_2 = \{b_1, b_2, \ldots, b_{n_2}\}$ respectively. If L_1 has n_2 parallel transversals then we can compose L_1 with L_2 to obtain a latin square L of order $n = n_1 + n_2$. Note that for any pair (n_1, n_2), there exists L_1 and L_2 with the above requirement, except for $(2,1)$, $(2,2)$, $(6,5)$ and $(6,6)$.

To produce L put L_1 and L_2 in the upper left and lower right corner respectively. Call the resulting square C_1, which looks as follows:

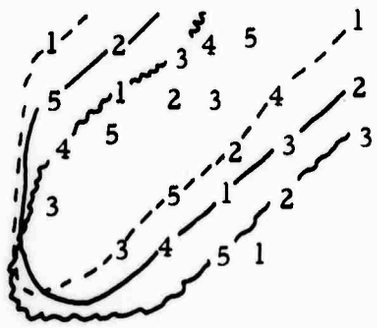
$$C_1 = \begin{array}{|c|c|}\hline L_1 & \\ \hline & L_2 \\ \hline \end{array}$$

Name the n_2 transversals of L_1 in any manner from 1 to n_2. Now fill the cell $(i, n_1 + k)$, $k = 1,2,\ldots,n_2$, with that element of transversal k which appears in row i, $i = 1,2,\ldots,n_1$. Fill also the cell $(n_1 + k, j)$, $k = 1,2,\ldots,n_2$,

with that element of transversal k which appears in column j, $j = 1,2,\ldots,n_1$. Call the resulting square C_2. Now every entry of C_2 is occupied with an element either from Σ_1 or Σ_2, but C_2 is obviously not a latin square on $\Sigma_1 \cup \Sigma_2$. However, if we replace each of the n_1 entries of transversal k with b_k, it is easily verified that the resulting square which we call L is a latin square of order n on $\Sigma_1 \cup \Sigma_2$.

The procedure described for filling the first n_1 entries of the row (column) $n_1 + k$ with the corresponding entries of transversal k is, naturally enough, called <u>the projection of transversal</u> k <u>on the first</u> n_1 <u>entries of row (column)</u> $n_1 + k$.

We shall now elucidate the above procedure via an example. Let $\Sigma_1 = \{1,2,3,4,5\}$, $\Sigma_2 = \{6,7,8\}$,

$L_1 =$ 

and $L_2 = \begin{matrix} 6 & 7 & 8 \\ 7 & 8 & 6 \\ 8 & 6 & 7 \end{matrix}$.

Note that the cells on the same curve in L_1 form a transversal.

$C_1 =$

1	2	3	4	5			
5	1	2	3	4			
4	5	1	2	3			
3	4	5	1	2			
2	3	4	5	1			
					6	7	8
					7	8	6
					8	6	7

and C_2

1	2	3	4	5	1	2	3
5	1	2	3	4	4	5	1
4	5	1	2	3	2	3	4
3	4	5	1	2	5	1	2
2	3	4	5	1	3	4	5
1	3	5	2	4	6	7	8
5	2	4	1	3	7	8	6
4	1	3	5	2	8	6	7

And finally

$$L = \left[\begin{array}{ccccc|ccc} 6 & 7 & 8 & 4 & 5 & 1 & 2 & 3 \\ 7 & 8 & 2 & 3 & 6 & 4 & 5 & 1 \\ 8 & 5 & 1 & 6 & 7 & 2 & 3 & 4 \\ 3 & 4 & 6 & 7 & 8 & 5 & 1 & 2 \\ 2 & 6 & 7 & 8 & 1 & 3 & 4 & 5 \\ \hline 1 & 3 & 5 & 2 & 4 & 6 & 7 & 8 \\ 5 & 2 & 4 & 1 & 3 & 7 & 8 & 6 \\ 4 & 1 & 3 & 5 & 2 & 8 & 6 & 7 \end{array}\right] .$$

which is a latin square of order 8 on $\Sigma_1 \cup \Sigma_2 = \{1,2,\ldots,8\}$.

Remark. Note that it is by no means required that the projection of transversals on the rows and columns should have the same ordering. Indeed, for the fixed set of ordered n_2 transversals, we have $n_2!$ choices of projections on columns and $n_2!$ choices of projections on the rows. Hence we can generate at least $(n_2!)^2$ different latin squares of order $n = n_1 + n_2$ composing L_1 and L_2.

XIII. 4. Construction of $O(n,2)$ Sets by Method of Sum Composition. In order to construct an $O(n,2)$ set for $n = n_1 + n_2$, we require that $n_1 \geq 2n_2$ and there should exist an $O(n_2,2)$ set, and an $O(n_1,2)$ set with $2n_2$ parallel transversals. It is easy to show that any $n \geq 10$ can be decomposed in at least one way into $n_1 + n_2$ which fulfill the above requirements. We now present two theorems which state that for certain n one can construct an $O(n,2)$ set by the method of sum composition.

Theorem XIII. 4.1. Let $n_1 = p^\alpha \geq 7$ for any odd prime p and positive integer α, excluding $n_1 = 13$. Then there exists an $O(n,2)$ set which can be constructed by composition of $O(n_1,2)$ and $O(n_2,2)$ sets for $n_2 = (n_1 - 1)/2$ and $n = n_1 + n_2$.

We shall first give the method of construction and then a proof that the constructed set is an $O(n,2)$ set.

Construction. Let $B(r)$ be the $n_1 \times n_1$ square with element $r\alpha_i + \alpha_j$ in its (i,j) cell, α_i, α_j, $0 \neq r$ in $GF(n_1)$, $i,j = 1,2,\ldots,n_1$. Then it is easy to see that $\{B(1), B(x), B(y)\}$, $y = x^{-1}$, $x \neq y$, is an $O(n_1,3)$ set. Consider the n_1 cells in $B(1)$ with $\alpha_i + \alpha_j = k$ a fixed element in $GF(n_1)$. Then the corresponding cells in $B(x)$ and $B(y)$ form a common transversal for the set $\{B(x), B(y)\}$. Name this common transversal by k. It is then obvious that two common transversals k_1 and k_2, $k_1 \neq k_2$ are parallel and hence $\{B(x), B(y)\}$ has n_1 common parallel transversals. Now let $\{A_1, A_2\}$ be any $O(n_2,2)$ set, which is known to exist, on a set Ω non-intersecting with $GF(n_1)$. For any λ in $GF(n_1)$ we can find $(n_1-1)/2$ pairs of distinct elements belonging to $GF(n_1)$ such that the sum of the two elements of each pair is equal to λ. Let $\{S\}$ and $\{T\}$ denote the collection of the first and the second elements of these $(n_1-1)/2$ pairs respectively. Note that for a fixed λ the set $\{S\}$ can be constructed in $(n_1-1)(n_1-3)\ldots 1$ distinct ways. Now fix λ and let L_1 denote any of the $(n_2!)^2$ latin squares that can be generated by the sum composition of $L(x)$ and A_1 using transversals determined by the n_2 elements of $\{S\}$. Let L_2 be the latin square derived from the composition of $L(y)$ and A_2 using the n_2 transversals determined by the elements of $\{T\}$ and the following projection rule: Project transversals t_i, $i = 1,2,\ldots,n_2$ on the row (column) which upon superposition of L_2 on L_1 this row (column) should coincide with the row (column) derived from the projection of the transversal $\lambda - t_i$. Shortly we shall prove that $\{L_1, L_2\}$ forms on $O(n,2)$ set.

The preceding arguments shows that $\{L_1, L_2\}$ can be constructed non-isomorphically in at least $(n_1-3)(n_2!)^2[n_1(n_1-1)(n_1-3)\ldots 1]$ ways. For instance in the case of $n_1 = 7$, there is at least 12096 non-isomorphic pairs of orthogonal latin squares of order 10. Therefore, Euler has been wrong in his conjecture by a very wide margin.

Note that we can construct infinitely many pairs of orthogonal latin squares of order $4t + 2$ by the method of theorem XIII. 4.1. For $p \equiv 7 \bmod 8$ and α odd $p^{\alpha} = (8t + 5)/3$. Hence $n_1 + n_2 = 4t + 2$.

Proof: The constructional procedure clearly reveals that:

A. L_1 and L_2 are latin squares of order n on $GF(n_1) \cup \Omega$.

B. Upon superposition of L_1 on L_2 the following are true:

b_1. Every element of Ω appears with every other element of Ω.

b_2. Every element of Ω appears with every element of $GF(n_1)$.

b_3. Every element of $GF(n_1)$ appears with every element of Ω.

Therefore, all we have to prove is that every element of $GF(n_1)$ appears with every other element of $GF(n_1)$. To prove this recall that $B(x)$ is orthogonal to $B(y)$. However, since we removed the n_2 transversals from $B(x)$ determined by the n_2 elements of $\{S\}$ and n_2 transversals from $B(y)$ determined by the n_2 elements of $\{T\}$ therefore the following $2n_2n_1$ pairs have been lost.

$$(x\alpha_i + \alpha_j,\ y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = \gamma \text{ for any } \gamma \in GF(n_1),\ \gamma \neq \lambda .$$

We claim that the given projection rules guarantee the capture of these lost pairs by the $2n_2n_1$ bordered cells. To show this note that the superposition of the

projected transversal s from $B(x)$ on the projected transversal $t = \lambda - s$ from $B(y)$ will capture the n_1 pairs

$$(x\alpha_i + \alpha_j,\ y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = k = [y(\lambda - s) + s]/(1 + y)$$

if these transversals have beer projected on row border and the n_1 pairs

$$(x\alpha_i + \alpha_j,\ y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = k = [s(y-1) + (s-\lambda)(x-1)]/(y-x)$$

if these transversals have been projected on column border. Now because $k + k' = \lambda$ and if $s_1 \neq s_2$ then $k_1 \neq k_2$ and $k_1' \neq k_2'$ hence the $2n_2n_1$ pairs which have been resulted from the projection of transversals determined by $\{S\}$ and $\{T\}$ will jointly capture the $2n_2n_1$ lost pairs and thus a proof.

We shall now clarify the above constructional procedure by an example.

Example. Let $n_1 = 7$, $GF(7) = \{0,1,2,\ldots,6\}$. Then for $x = 2$, $y = x^{-1} = 4$ we have

$\{B(1), B(2), B(4)\} =$

0 1 2 3 4 5 6	0 1 2 3 4 5 6	0 1 2 3 4 5 6
1 2 3 4 5 6 0	2 3 4 5 6 0 1	4 5 6 0 1 2 3
2 3 4 5 6 0 1	4 5 6 0 1 2 3	1 2 3 4 5 6 0
3 4 5 6 0 1 2	6 0 1 2 3 4 5	5 6 0 1 2 3 4
4 5 6 0 1 2 3	1 2 3 4 5 6 0	2 3 4 5 6 0 1
5 6 0 1 2 3 4	3 4 5 6 0 1 2	6 0 1 2 3 4 5
6 0 1 2 3 4 5	5 6 0 1 2 3 4	3 4 5 6 0 1 2

For $n_2 = (n_1-1)/2 = 3$ let $\Omega_2 = \{7,8,9\}$ and

$\{A_1, A_2\} =$ $\begin{matrix} 7 & 8 & 9 & 7 & 8 & 9 \\ 8 & 9 & 7, & 9 & 7 & 8 \\ 9 & 7 & 8 & 8 & 9 & 7 \end{matrix}$. Finally for $\lambda = 0$, $\{S\} = \{1,2,3\}$ and $\{T\} = \{6,5,4\}$ we have $\{L_1, L_2\} =$

0	7	8	9	4	5	6	1	2	3	0	1	2	3	7	8	9	6	5	4
7	8	9	5	6	0	1	2	3	4	4	5	6	7	8	9	3	2	1	0
8	9	6	0	1	2	7	3	4	5	1	2	7	8	9	6	0	5	4	3
9	0	1	2	3	7	8	4	5	6	5	7	8	9	2	3	4	1	0	6
1	2	3	4	7	8	9	5	6	0	7	8	9	5	6	0	1	4	3	2
3	4	5	7	8	9	2	6	0	1	8	9	1	2	3	4	7	0	6	5
5	6	7	8	9	3	4	0	1	2	9	4	5	6	0	7	8	3	2	1
2	1	0	6	5	4	3	7	8	9	3	0	4	1	5	2	6	7	8	9
4	3	2	1	0	6	5	8	9	7	6	3	0	4	1	5	2	9	7	8
6	5	4	3	2	1	0	9	7	8	2	6	3	0	4	1	5	8	9	7

the reader can easily verify that $\{L_1, L_2\}$ is an $O(10,2)$ set.

Remarks.

1) The method of theorem XIII. 4.1 fails for $n_1 = 13$ only because there is no $O(6,2)$ set. Otherwise, there will be no orthogonality contradiction on the other parts of L_1 and L_2 with their 6×6 lower right square missing.

2) In the case of $n_1 = 7$, if we let $\{S\} = \{0,1,3\}$ and $\{T\} = \{2,4,5\}$ then the requirement $y = x^{-1}$ is not necessary. However then we do not have a unified projection rule for the formation of L_2 as was provided for the case $y = x^{-1}$ by theorem XIII. 4. 1. To give the complete list of solutions let (a_1,a_2,a_3) and (b_1,b_2,b_3) be any two permutations of the set $\{8,9,10\}$. If we project transversals $(0,1,3)$ on the rows (a_1,a_2,a_3) and columns (b_1,b_2,b_3) in the formation of L_1, then the following table indicates what permutation of transversals $\{2,4,5\}$ should be projected on the rows (a_1,a_2,a_3) and columns (b_1,b_2,b_3) in the formation of L_2. Obviously these permutations will be a function of the pair (x,y).

Pair (x,y)	Rows a_1, a_2, a_3	Columns b_1, b_2, b_3
(2,3)	4, 2, 5	4, 2, 5
(2,3)	2, 5, 4	2, 5, 4
(2,4)	2, 5, 4	4, 2, 5
(2,5)	4, 2, 5	4, 2, 5
(2,6)	2, 5, 4	2, 5, 4
(3,4)	2, 5, 4	2, 5, 4
(3,5)	2, 5, 4	4, 2, 5
(3,5)	4, 2, 5	5, 4, 2
(3,5)	4, 2, 5	2, 5, 4
(3,5)	5, 4, 2	2, 5, 4
(3,6)	4, 2, 5	2, 5, 4
(3,6)	5, 4, 2	4, 2, 5
(4,5)	2, 5, 4	2, 5, 4
(4,6)	5, 4, 2	4, 2, 5
(4,6)	2, 5, 4	2, 5, 4
(4,6)	5, 4, 2	5, 4, 2

(This table is by no means exhaustive.)

The reader may note that whenever $y = x^{-1}$ in the above table the given solution(s) are different from the one provided by the method of theorem XIII. 4. 1.

Thus we can conclude that any pair of orthogonal latin squares of order 7 based on the GF(7) can be composed with a pair of orthogonal latin squares of

order 3 and make a pair of orthogonal latin squares of order 10 . In addition, since we have six choices for (a_1,a_2,a_3) and (b_1,b_2,b_3) hence from every line in the above table we can produce 36 non-isomorphic $O(10,2)$ sets or $16 \times 36 = 576$ sets for the entire table. Since all these pairs are non-isomorphic with all previous pairs, produced by theorem XIII.4.1, thus by the method of sum composition one can at least produce 12,672 non-isomorphic $O(10,2)$ sets.

We believe that for other values of n_1 there are sets of $\{S\}$ and $\{T\}$ together with proper projections which makes the restriction $y = x^{-1}$ unnecessary.

Theorem XIII.4.2. Let $n_1 = 2^\alpha \geq 8$ for any positive integer α. Then there exists an $O(n,2)$ set which can be constructed by composition of $O(n_1,2)$ and $O(n_2,2)$ sets for $n_2 = n_1/2$ and $n = n_1 + n_2$.

We shall here give only the method of construction. A similar argument as in theorem XIII.4.1 will show that the constructed set is an $O(n,2)$ set.

Construction. In a similar fashion as in theorem XIII.4.1 construct the set $\{B(1), B(x), B(y)\}$ over $GF(2^\alpha)$. Let also $\{A_1,A_2\}$ be any $O(n_2,2)$ set, which always exists, on a set Ω non-intersecting with $GF(2^\alpha)$. For any $\lambda \neq 0$ in $GF(2^\alpha)$ we can find $n_1/2$ pairs of distinct elements belonging to $GF(2^\alpha)$ such that the sum of the two elements of each pair is equal to λ . Let $\{S\}$ and $\{T\}$ denote the collection of the first and the second elements of these $n_1/2$ pairs respectively. Note that for a fixed λ the set $\{S\}$ can be constructed in $n_1(n_1-2)(n_1-4)\ldots 1$ distinct ways. Now form L_1 from the sum composition of $B(x)$ and A_1 and L_2 from the sum composition of $B(y)$ and A_2 using the same projection rule as given in theorem XIII.4.1. Now $\{L_1,L_2\}$ is an $O(n,2)$ set.

Example. Let $n = 8$, $GF(8) = \{0,1,2,\ldots,7\}$ with the following addition (+) and multiplication (×) tables:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	6	4	3	7	2	5
2	2	6	0	7	5	4	1	3
3	3	4	7	0	1	6	5	2
4	4	3	5	1	0	2	7	6
5	5	7	4	6	2	0	3	1
6	6	2	1	5	7	3	0	4
7	7	5	3	2	6	1	4	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	3	4	5	6	7	1
3	0	3	4	5	6	7	1	2
4	0	4	5	6	7	1	2	3
5	0	5	6	7	1	2	3	4
6	0	6	7	1	2	3	4	5
7	0	7	1	2	3	4	5	6

Then for $x = 2$, $y = x^{-1} = 7$ we have

$\{B(1), B(2), B(7)\} =$

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
1 0 6 4 3 7 2 5	2 6 0 7 5 4 1 3	7 5 3 2 6 1 4 0
2 6 0 7 5 4 1 3	3 4 7 0 1 6 5 2	1 0 6 4 3 7 2 5
3 4 7 0 1 6 5 2	4 3 5 1 0 2 7 6	2 6 0 7 5 4 1 3
4 3 5 1 0 2 7 6	5 7 4 6 2 0 3 1	3 4 7 0 1 6 5 2
5 7 4 6 2 0 3 1	6 2 1 5 7 3 0 4	4 3 5 1 0 2 7 6
6 2 1 5 7 3 0 4	7 5 3 2 6 1 4 0	5 7 4 6 2 0 3 1
7 5 3 2 6 1 4 0	1 0 6 4 3 7 2 5	6 2 1 5 7 3 0 4

For $n_2 = n_1/2 = 4$ let $\Omega = \{A,B,C,D\}$ and

$$\{A_1,A_2\} = \begin{array}{cc} \begin{array}{cccc} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{array} & \begin{array}{cccc} A & B & C & D \\ D & C & B & A \\ B & A & D & C \\ C & D & A & B \end{array} \end{array}$$

Finally for $\lambda = 5$, $\{S\} = \{0,1,3,4\}$ and $\{T\} = \{5,7,6,2\}$ we have $\{L_1,L_2\} =$

A B 2 C D 5 6 7 | 0 1 3 4	0 1 D 3 4 A C B | 5 7 6 2
B A 0 D C 4 1 3 | 6 2 5 7	7 5 C 2 6 B D A | 0 1 3 4
3 4 A 0 1 D B C | 7 5 2 6	D C 6 B A 7 2 5 | 3 4 0 1
C D 5 A B 2 7 6 | 1 0 4 3	2 6 B 7 5 C A D | 1 0 4 3
D C 4 B A 0 3 1 | 2 6 7 5	3 4 A 0 1 D B C | 7 5 2 6
6 2 D 5 7 A C B | 3 4 0 1	A B 5 C D 2 7 6 | 4 3 1 0
7 5 B 2 6 C A D | 4 3 1 0	C D 4 A B 0 3 1 | 6 2 5 7
1 0 C 4 3 B D A | 5 7 6 2	B A 1 D C 3 0 4 | 2 6 7 5
0 6 7 1 2 3 4 5 | A B C D	4 2 7 6 3 5 1 0 | A B C D
2 1 3 6 0 7 5 4 | B A D C	6 3 0 4 2 1 5 7 | D C B A
4 7 6 3 5 1 0 2 | C D A B	5 0 3 1 7 4 6 2 | B A D C
5 3 1 7 4 6 2 0 | D C B A	1 7 2 5 0 6 4 3 | C D A B

which is an $O(12,2)$ set.

Discussion. The necessary requirements for the construction of an $O(n,t)$ set, $n = n_1 + n_2$, $t < n_2$, by the method of sum composition are: The existence of an $O(n_1,t)$ set, $n_1 \geq tn_2$, with at least tn_2 common parallel transversals, and an $O(n_2,t)$ set. These conditions are obviously satisfied whenever n_1 and n_2 are prime powers.

While for some values of n there exists only a unique decomposition fulfilling the above requirements, for infinitely many other values of n there are abundant such decompositions.

It seems that if there exists an $O(n_2,2)$ set and if $n = n_1 + n_2$, $n_1 \geq 2n_2$ then one can construct an $O(n,2)$ set by the method of sum composition if n_1 is a prime power. To support this observation and shed some more light on the method of sum composition we present in subsequent pages some highlights of the results which we hope to complete and submit for publication shortly.

In the following for each given decomposition of n we exhibit an $O(n,2)$ set which has been derived by the method of sum composition. We shall represent the pairs in a form that the curious reader can easily reconstruct the original sets. Hereafter the notation $L_1 \perp L_2$ means that L_1 is orthogonal to L_2.

1) $12 = 9 + 3$

A	B	C	4	5	6	7	8	9	1	2	3
B	C	A	1	2	3	4	5	6	9	7	8
C	A	B	7	8	9	1	2	3	5	6	4
2	3	1	5	6	4	A	B	C	8	9	7
8	9	7	2	3	1	B	C	A	4	5	6
5	6	4	8	9	7	C	A	B	3	1	2
3	1	2	A	B	C	9	7	8	6	4	5
9	7	8	B	C	A	6	4	5	2	3	1
6	4	5	C	A	B	3	1	2	7	8	9
1	5	9	6	7	2	8	3	4	A	B	C
7	2	6	3	4	8	5	9	1	B	C	A
4	8	3	9	1	5	2	6	7	C	A	B

$\perp$

1	2	3	4	5	6	A	B	C	8	9	7
9	7	8	3	1	2	B	C	A	6	4	5
5	6	4	8	9	7	C	A	B	1	2	3
6	4	5	A	B	C	3	1	2	7	8	9
2	3	1	B	C	A	8	9	7	5	6	4
7	8	9	C	A	B	4	5	6	3	1	2
A	B	C	2	3	1	5	6	4	9	7	8
B	C	A	7	8	9	1	2	3	4	5	6
C	A	B	6	4	5	9	7	8	2	3	1
4	9	2	5	7	3	6	8	1	A	B	C
3	5	7	1	6	8	2	4	9	C	A	B
8	1	6	9	2	4	7	3	5	B	C	A

2) $14 = 11 + 3$, the only decomposition which fulfills the necessary requirements.

A	B	C	3	4	5	6	7	8	9	10	0	1	2
B	C	9	10	0	1	2	3	4	5	A	6	7	8
C	4	5	6	7	8	9	10	0	A	B	1	2	3
10	0	1	2	3	4	5	6	A	B	C	7	8	9
6	7	8	9	10	0	1	A	B	C	5	2	3	4
2	3	4	5	6	7	A	B	C	0	1	8	9	10
9	10	0	1	2	A	B	C	6	7	8	3	4	5
5	6	7	8	A	B	C	1	2	3	4	9	10	0
1	2	3	A	B	C	7	8	9	10	0	4	5	6
8	9	A	B	C	2	3	4	5	6	7	10	0	1
4	A	B	C	8	9	10	0	1	2	3	5	6	7
0	5	10	4	9	3	8	2	7	1	6	A	B	C
7	1	6	0	5	10	4	9	3	8	2	B	C	A
3	8	2	7	1	6	0	5	10	4	9	C	A	B

0	1	2	3	4	5	6	7	A	B	C	9	10	8
8	9	10	0	1	2	3	A	B	C	7	5	6	4
5	6	7	8	1	10	A	B	C	3	4	1	2	0
2	3	4	5	6	A	B	C	10	0	1	8	9	7
10	0	1	2	A	B	C	6	7	8	9	4	5	3
7	8	9	A	B	C	2	3	4	5	6	0	1	10
4	5	A	B	C	9	10	0	1	2	3	7	8	6
1	A	B	C	5	6	7	8	9	10	0	3	4	2
A	B	C	1	2	3	4	5	6	7	8	10	0	9
B	C	8	9	10	0	1	2	3	4	A	6	7	5
C	4	5	6	7	8	9	10	0	A	B	2	3	1
6	10	3	7	0	4	8	1	5	9	2	A	B	C
3	7	0	4	8	1	5	9	2	6	10	C	A	B
9	2	6	10	3	7	0	4	8	1	5	B	C	A

3) $15 = 12 + 3$, $15 = 11 + 4$ are the only decompositions which fulfill the necessary requirements. However, we consider here the latter decomposition since we can utilize the properties of Galois field GF(11).

A	B	C	D	4	5	6	7	8	9	10	0	1	2	3
B	C	D	5	6	7	8	9	10	0	A	1	2	3	4
C	D	6	7	8	9	10	0	1	A	B	2	3	4	5
D	7	8	9	10	0	1	2	A	B	C	3	4	5	6
8	9	10	0	1	2	3	A	B	C	D	4	5	6	7
10	0	1	2	3	4	A	B	C	D	9	5	6	7	8
1	2	3	4	5	A	B	C	D	10	0	6	7	8	9
3	4	5	6	A	B	C	D	0	1	2	7	8	9	10
5	6	7	A	B	C	D	1	2	3	4	8	9	10	0
7	8	A	B	C	D	2	3	4	5	6	9	10	0	1
9	A	B	C	D	3	4	5	6	7	9	10	0	1	2
0	10	9	8	7	6	5	4	3	2	1	A	B	C	D
2	1	0	10	9	8	7	6	5	4	3	B	A	D	C
4	3	2	1	0	10	9	8	7	6	5	C	D	A	B
6	5	4	3	2	1	0	10	9	8	7	D	C	B	A

$\perp$

0	1	2	3	4	5	A	B	C	D	10	8	6	9	7
6	7	8	9	10	A	B	C	D	4	5	2	0	3	1
1	2	3	4	A	B	C	D	9	10	0	7	5	8	6
7	8	9	A	B	C	D	3	4	5	6	1	10	2	0
2	3	A	B	C	D	8	9	10	0	1	6	4	7	5
8	A	B	C	D	2	3	4	5	6	7	0	9	1	10
A	B	C	D	7	8	9	10	0	1	2	5	3	6	4
B	C	D	1	2	3	4	5	6	7	A	10	8	0	9
C	D	6	7	8	9	10	0	1	A	B	4	2	5	3
D	0	1	2	3	4	5	6	A	B	C	9	7	10	8
5	6	7	8	9	10	0	A	B	C	D	3	1	4	2
9	4	10	5	0	6	1	7	2	8	3	A	B	C	D
10	5	0	7	1	7	2	8	3	9	4	D	C	B	A
3	9	4	10	5	0	6	1	7	2	8	B	A	D	C
4	10	5	0	6	1	7	2	8	3	9	C	D	A	B

4) $17 = 13 + 4$ and $17 = 12 + 5$ are the only decompositions which fulfill the necessary requirements. The following pair is derived through the first decomposition.

A	B	C	D	4	5	6	7	8	9	10	11	12	0	1	2	3
B	C	D	8	9	10	11	12	0	1	2	3	A	4	5	6	7
C	D	12	0	1	2	3	4	5	6	7	A	B	8	9	10	11
D	3	4	5	6	7	8	9	10	11	A	B	C	12	0	1	2
7	8	9	10	11	12	0	1	2	A	B	C	D	3	4	5	6
12	0	1	2	3	4	5	6	A	B	C	D	11	7	8	9	10
4	5	6	7	8	9	10	A	B	C	D	2	3	11	12	0	1
9	10	11	12	0	1	A	B	C	D	6	7	8	2	3	4	5
1	2	3	4	5	A	B	C	D	10	11	12	0	6	7	8	9
6	7	8	9	A	B	C	D	1	2	3	4	5	10	11	12	0
11	12	0	A	B	C	D	5	6	7	8	9	10	1	2	3	4
3	4	A	B	C	D	9	10	11	12	0	1	2	5	6	7	8
8	A	B	C	D	0	1	2	3	4	5	6	7	9	10	11	12
0	9	5	1	10	6	2	11	7	3	12	8	4	A	B	C	D
5	1	10	6	2	11	7	3	12	8	4	0	9	B	A	D	C
10	6	2	11	7	3	12	8	4	0	9	5	1	C	D	A	B
2	11	7	3	12	8	4	0	9	5	1	10	6	D	C	B	A

$\perp$

0	1	2	3	4	5	6	7	A	B	C	D	12	9	8	11	10
8	9	10	11	12	0	1	A	B	C	D	6	7	3	2	5	4
3	4	5	6	7	8	A	B	C	D	0	1	2	10	9	12	7
11	12	0	1	2	A	B	C	D	7	8	9	10	4	3	6	5
6	7	8	9	A	B	C	D	1	2	3	4	5	11	10	0	12
1	2	3	A	B	C	D	8	9	10	11	12	0	5	4	7	6
9	10	A	B	C	D	2	3	4	5	6	7	8	12	11	1	0
4	A	B	C	D	9	10	11	12	0	1	2	3	6	5	8	7
A	B	C	D	3	4	5	6	7	8	9	10	11	0	12	2	1
B	C	D	10	11	12	0	1	2	3	4	5	A	7	6	9	8
C	D	4	5	6	7	8	9	10	11	12	A	B	1	0	3	2
D	11	12	0	1	2	3	4	5	6	A	B	C	8	7	10	9
5	6	7	8	9	10	11	12	0	A	B	C	D	2	1	4	3
7	0	6	12	5	11	4	10	3	9	2	8	1	A	B	C	D
12	5	11	4	10	3	9	2	8	1	7	0	6	D	C	B	A
10	3	9	2	8	1	7	0	6	12	5	11	4	B	A	D	C
2	8	1	7	0	6	12	5	11	4	10	3	9	C	D	A	B

5) We do not know if an O(14,2) set with 8 common parallel transversals exists or if an O(15,2) set with 6 common transversals corresponding to the O(15,3) set in section V can be combined with an O(3,2) set to form an O(18,2) set. Therefore, the following O(18,2) set is constructed from the decomposition 18 = 13 + 5 .

A	B	C	D	E	5	6	7	8	9	10	11	12	0	1	2	3	4
B	C	D	E	6	7	8	9	10	11	12	0	A	1	2	3	4	5
C	D	E	7	8	9	10	11	12	0	1	A	B	2	3	4	5	6
D	E	8	9	10	11	12	0	1	2	A	B	C	3	4	5	6	7
E	9	10	11	12	0	1	2	3	A	B	C	D	4	5	6	7	8
10	11	12	0	1	2	3	4	A	B	C	D	E	5	6	7	8	9
12	0	1	2	3	4	5	A	B	C	D	E	11	6	7	8	9	10
1	2	3	4	5	6	A	B	C	D	E	12	0	7	8	9	10	11
3	4	5	6	7	A	B	C	D	E	0	1	2	8	9	10	11	12
5	6	7	8	A	B	C	D	E	1	2	3	4	9	10	11	12	0
7	8	9	A	B	C	D	E	2	3	4	5	6	10	11	12	0	1
9	10	A	B	C	D	E	3	4	5	6	7	8	11	12	0	1	2
11	A	B	C	D	E	4	5	6	7	8	9	10	12	0	1	2	3
0	12	11	10	9	8	7	6	5	4	3	2	1	A	B	C	D	E
2	1	0	12	11	10	9	8	7	6	5	4	3	B	C	D	E	A
4	3	2	1	0	12	11	10	9	8	7	6	5	C	D	E	A	B
6	5	4	3	2	1	0	12	11	10	9	8	7	D	E	A	B	C
8	7	6	5	4	3	2	1	0	12	11	10	9	E	A	B	C	D

⊥

0	1	2	3	4	5	6	A	B	C	D	E	12	7	9	10	11	8
7	8	9	10	11	12	A	B	C	D	E	5	6	0	2	3	4	1
1	2	3	4	5	A	B	C	D	E	11	12	0	6	8	9	10	7
8	9	10	11	A	B	C	D	E	4	5	6	7	12	1	2	3	0
2	3	4	A	B	C	D	E	10	11	12	0	1	5	7	8	9	6
9	10	A	B	C	D	E	3	4	5	6	7	8	11	0	1	2	12
3	A	B	C	D	E	9	10	11	12	0	1	2	4	6	7	8	5
A	B	C	D	E	2	3	4	5	6	7	8	9	10	12	0	1	11
B	C	D	E	8	9	10	11	12	0	1	2	A	3	5	6	7	4
C	D	E	1	2	3	4	5	6	7	8	A	B	9	11	12	0	10
D	E	7	8	9	10	11	12	0	1	A	B	C	2	4	5	6	3
E	0	1	2	3	4	5	6	7	A	B	C	D	8	10	11	12	9
6	7	8	9	10	11	12	0	A	B	C	D	E	1	3	4	5	2
4	11	5	12	6	0	7	1	8	2	9	3	10	A	B	C	D	E
12	6	0	7	1	8	2	9	3	10	4	11	5	E	A	B	C	D
10	4	11	5	12	6	0	7	1	8	2	9	3	D	E	A	B	C
5	12	6	0	7	1	8	2	9	3	10	4	11	C	D	E	A	B
11	5	12	6	0	7	1	8	2	9	3	10	4	B	C	D	E	A

6) We do not know if an O(15,2) set with 14 common parallel transversals corresponding to the O(15,3) set in section V can be combined with an O(7,2) set to form an O(22,2) set or if there exists an O(18,2) set with 8 common parallel transversals. Therefore, the following O(22,2) sets are derived from the decompositions 22 = 19 + 3 and 22 = 17 + 5 .

a: 22 = 19 + 3,

A	B	C	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2
B	C	5	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	A	2	3	4
C	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	A	B	4	5	6
9	10	11	12	13	14	15	16	17	18	0	1	2	3	4	5	A	B	C	6	7	8
12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	A	B	C	11	8	9	10
15	16	17	18	0	1	2	3	4	5	6	7	8	9	A	B	C	13	14	10	11	12
18	0	1	2	3	4	5	6	7	8	9	10	11	A	B	C	15	16	17	12	13	14
2	3	4	5	6	7	8	9	10	11	12	13	A	B	C	17	18	0	1	14	15	16
5	6	7	8	9	10	11	12	13	14	15	A	B	C	0	1	2	3	4	16	17	18
8	9	10	11	12	13	14	15	16	17	A	B	C	2	3	4	5	6	7	18	0	1
11	12	13	14	15	16	17	18	0	A	B	C	4	5	6	7	8	9	10	1	2	3
14	15	16	17	18	0	1	2	A	B	C	6	7	8	9	10	11	12	13	3	4	5
17	18	0	1	2	3	4	A	B	C	8	9	10	11	12	13	14	15	16	5	6	7
1	2	3	4	5	6	A	B	C	10	11	12	13	14	15	16	17	18	0	7	8	9
4	5	6	7	8	A	B	C	12	13	14	15	16	17	18	0	1	2	3	9	10	11
7	8	9	10	A	B	C	14	15	16	17	18	0	1	2	3	4	5	6	11	12	13
10	11	12	A	B	C	16	17	18	0	1	2	3	4	5	6	7	8	9	13	14	15
13	14	A	B	C	18	0	1	2	3	4	5	6	7	8	9	10	11	12	15	16	17
16	A	B	C	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	17	18	0
0	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2	A	B	C
3	1	18	16	14	12	10	8	6	4	2	0	17	15	13	11	9	7	5	B	C	A
5	4	2	0	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	C	A	B

0	1	2	3	4	5	6	7	8	9	10	11	12	A	B	C	16	17	18	14	15	13
13	14	15	16	17	18	0	1	2	3	4	5	A	B	C	9	10	11	12	7	8	6
7	8	9	10	11	12	13	14	15	16	17	A	B	C	2	3	4	5	6	0	1	18
1	2	3	4	5	6	7	8	9	10	A	B	C	14	15	16	17	18	0	12	13	11
14	15	16	17	18	0	1	2	3	A	B	C	7	8	9	10	11	12	13	5	6	4
8	9	10	11	12	13	14	15	A	B	C	0	1	2	3	4	5	6	7	17	18	16
2	3	4	5	6	7	8	A	B	C	12	13	14	15	16	17	18	0	1	10	11	9
15	16	17	18	0	1	A	B	C	5	6	7	8	9	10	11	12	13	14	3	4	2
9	10	11	12	13	A	B	C	17	18	0	1	2	3	4	5	6	7	8	15	16	14
3	4	5	6	A	B	C	10	11	12	13	14	15	16	17	18	0	1	2	8	9	7
16	17	18	A	B	C	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	0
10	11	A	B	C	15	16	17	18	0	1	2	3	4	5	6	7	8	9	13	14	12
4	A	B	C	8	9	10	11	12	13	14	15	16	17	18	0	1	2	3	6	7	5
A	B	C	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	18	0	17
B	C	13	14	15	16	17	18	0	1	2	3	4	5	6	7	8	9	A	11	12	10
C	6	7	8	9	10	11	12	13	14	15	16	17	18	0	1	2	A	B	4	5	3
18	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	A	B	C	16	17	15
12	13	14	15	16	17	18	0	1	2	3	4	5	6	7	A	B	C	11	9	10	8
6	7	8	9	10	11	12	13	14	15	16	17	18	0	A	B	C	4	5	2	3	1
11	18	6	13	1	8	15	3	10	17	5	12	0	7	14	2	9	16	4	A	B	C
5	12	0	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	C	A	B
17	5	12	0	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	B	C	A

b: $22 = 17 + 5$,

A	B	C	D	E	5	6	7	8	9	10	11	12	13	14	15	16	0	1	2	3	4
B	C	D	E	6	7	8	9	10	11	12	13	14	15	16	0	A	1	2	3	4	5
C	D	E	7	8	9	10	11	12	13	14	15	16	0	1	A	B	2	3	4	5	6
D	E	8	9	10	11	12	13	14	15	16	0	1	2	A	B	C	3	4	5	6	7
E	9	10	11	12	13	14	15	16	0	1	2	3	A	B	C	D	4	5	6	7	8
10	11	12	13	14	15	16	0	1	2	3	4	A	B	C	D	E	5	6	7	8	9
12	13	14	15	16	0	1	2	3	4	5	A	B	C	D	E	11	6	7	8	9	10
14	15	16	0	1	2	3	4	5	6	A	B	C	D	E	12	13	7	8	9	10	11
16	0	1	2	3	4	5	6	7	A	B	C	D	E	13	14	15	8	9	10	11	12
1	2	3	4	5	6	7	8	A	B	C	D	E	14	15	16	0	9	10	11	12	13
3	4	5	6	7	8	9	A	B	C	D	E	15	16	0	1	2	10	11	12	13	14
5	6	7	8	9	10	A	B	C	D	E	16	0	1	2	3	4	11	12	13	14	15
7	8	9	10	11	A	B	C	D	E	0	1	2	3	4	5	6	12	13	14	15	16
9	10	11	12	A	B	C	D	E	1	2	3	4	5	6	7	8	13	14	15	16	0
11	12	13	A	B	C	D	E	2	3	4	5	6	7	8	9	10	14	15	16	0	1
13	14	A	B	C	D	E	3	4	5	6	7	8	9	10	11	12	15	16	0	1	2
15	A	B	C	D	E	4	5	6	7	8	9	10	11	12	13	14	16	0	1	2	3
0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	A	B	C	D	E
2	1	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	B	C	D	E	A
4	3	2	1	0	16	15	14	13	12	11	10	9	8	7	6	5	C	D	E	A	B
6	5	4	3	2	1	0	16	15	14	13	12	11	10	9	8	7	D	E	A	B	C
8	7	6	5	4	3	2	1	0	16	15	14	13	12	11	10	9	E	A	B	C	D

0	1	2	3	4	5	6	7	8	A	B	C	D	E	14	15	16	10	11	12	13	9
9	10	11	12	13	14	15	16	A	B	C	D	E	5	6	7	8	1	2	3	4	0
1	2	3	4	5	6	7	A	B	C	D	E	13	14	15	16	0	9	10	11	12	8
10	11	12	13	14	15	A	B	C	D	E	4	5	6	7	8	9	0	1	2	3	16
2	3	4	5	6	A	B	C	D	E	12	13	14	15	16	0	1	8	9	10	11	7
11	12	13	14	A	B	C	D	E	3	4	5	6	7	8	9	10	16	0	1	2	15
3	4	5	A	B	C	D	E	11	12	13	14	15	16	0	1	2	7	8	9	10	6
12	13	A	B	C	D	E	2	3	4	5	6	7	8	9	10	11	15	16	0	1	14
4	A	B	C	D	E	10	11	12	13	14	15	16	0	1	2	3	6	7	8	9	5
A	B	C	D	E	1	2	3	4	5	6	7	8	9	10	11	12	14	15	16	0	13
B	C	D	E	9	10	11	12	13	14	15	16	0	1	2	3	A	5	6	7	8	4
C	D	E	0	1	2	3	4	5	6	7	8	9	10	11	A	B	13	14	15	16	12
D	E	8	9	10	11	12	13	14	15	16	0	1	2	A	B	C	4	5	6	7	3
E	16	0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	12	13	14	15	11
7	8	9	10	11	12	13	14	15	16	0	1	A	B	C	D	E	3	4	5	6	2
16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	15	11	12	13	14	10
8	9	10	11	12	13	14	15	16	0	A	B	C	D	E	6	7	2	3	4	5	1
5	14	6	15	7	16	8	0	9	1	10	2	11	3	12	4	13	A	B	C	D	E
14	6	15	7	16	8	0	9	1	10	2	11	3	12	4	13	5	E	A	B	C	D
6	15	7	16	8	0	9	1	10	2	11	3	12	4	13	5	14	D	E	A	B	C
15	7	16	8	0	9	1	10	2	11	3	12	4	13	5	14	6	C	D	E	A	B
13	5	14	6	15	7	16	8	0	9	1	10	2	11	3	12	4	B	C	D	E	A

XIV. Computer Construction of O(10, t) Sets

In about fifteen years the effectiveness of computers in searching for orthogonal sets of latin squares of order ten has increased strikingly. Still the problem is so large that there seems to be little reason for optimism that the order ten problem can be completed by computers. More precisely, if (as most conversant with the problem consider quite plausible) no $O(10,3)$ set of orthogonal latin squares of order ten exists, then the number of cases to consider seems too large for an exhaustive proof by computer to be achievable. The number of latin squares of order ten is astronomical.

About 1953 Paige and Tompkins [1960] programmed SWAC to search for squares orthogonal to a fixed latin square of order ten. A few hours of running produced no orthogonal square, and was regarded as a bit of experimental evidence for the truth of Euler's conjecture. Calculations based on the progress made in the search led to the extrapolation that over fifty million years of computer time would be required to search for all squares orthogonal to a latin square of order ten put into SWAC intially. (At about the same time a similar program was written and similar results obtained with MANIAC at Los Alamos; this attempt has not been reported in print.)

In 1959, after Euler's conjecture had been disproved for all orders $4t + 2 > 6$, Parker programmed UNIVAC 1206 to search for squares orthogonal to a latin square of order ten. The running time was sharply less than for SWAC or MANIAC, about thirty minutes for the majority of latin squares. This was accomplished by generating and storing all transversals of the input latin square,

then searching for all ways to form latin squares from the list of transversals. (A transversal, or directrix, is a set of cells of a latin square, one in each row, one in each column, and one containing each digit.) The striking gain in speed over the earlier efforts occurred largely because the number of transversals of a typical latin square of order ten is roughly 850, much less than 10!; and, of course, the search was several levels deep. (SWAC and MANIAC were programmed to build up starts of latin squares toward orthogonal mates by filling in cells to form rows.)

There were two main outcomes from considerable running of Parker's 1206 program: 1) O(10,3) sets of latin squares are not numerous; more precisely, only a small fraction, if any, order ten squares could possibly extend to O(10,3) sets. Some 400 latin squares were run. Some were random, some were computer output fed back as input and hence known to have an orthogonal mate, and some were considered interesting candidates for intuitive reasons by Parker and others. Not once did an exhaustive search for orthogonal mates of an input latin square discover a pair orthogonal to one another. Mild evidence may be claimed supporting the opinion that no O(10,3) set exists. 2) Of a computer-generated sample of 100 random latin squares of order ten (program by R. T. Ostrowski), 62 have orthogonal mates. Thus, unlike O(10,3) sets, O(10,2) sets of squares are quite common. Euler's intuition for order ten was not only wrong, but in this sense wrong by a large margin. It was this finding which tempted Parker for a time to believe that repeated runs of the program should have a good chance of producing at an O(10,3) set, but many failures dimmed this optimism.

In 1967 John W. Brown programmed IBM 7094 to decide whether an input latin square of order ten can be extended to an $O(10,3)$ set. The running time was one half minute. Almost needless to say, transversals again were generated. Searching for patterns of transversals toward extension to an $O(10,3)$ set produced a speed gain over the previous program for orthogonal pairs. Brown endeavored to get every drop of speed from the machine. As before, hundreds of input order-ten latin squares produced no $O(10,3)$ set.

XV. On the Equivalence of O(n, t) Sets With Other Combinatorial Systems

XV. 0. Summary

In this section we have densely summarized some of the results obtained by author and at least fourteen others in order to demonstrate the importance of the theory of mutually orthogonal latin squares. We have shown that fourteen well-known and important combinatorial systems with certain parameters are actually equivalent to a set of mutually orthogonal latin squares. A schematic representation of these equivalences has been demonstrated in four wheels which we have called "Fundamental Wheels of Combinatorial Mathematics".

XV. 1. Introduction

The theory of mutually orthogonal latin squares owes its importance to the fact that many well-known combinatorial systems are actually equivalent to a set of mutually orthogonal latin squares; viz., finite projective plane, finite Euclidean plane, net, BIB, PBIB, orthogonal arrays, a set of mutually orthogonal matrices, error correcting codes, strongly regular graphs, complete graphs, a balanced set of ℓ-restrictional lattice designs, difference sets, Hadamard matrices, and an arrangement of non attacking rooks on hyperdimensional chess board. These combinatorial systems are unquestionably potent and effective in all branches of combinatorial mathematics, and in particular, in the construction of experimental designs. Therefore, a statement that the theory of mutually orthogonal latin squares is perhaps the most important theory in the field of experiment designs is not in the least exaggerated as far as this author is concerned.

Our purpose in this section is to demonstrate the relation of a set of mutually orthogonal latin squares with the above mentioned combinatorial systems. We shall present the essence of the known results available only in scattered literature in one theorem which we consider to be a "fundamental theorem of combinatorial mathematics". For the definitions of these combinatorial systems and the proof of the forthcoming theorem see the list of references given at the end of this paper.

XV. 2. Notation

For the sake of conciseness we introduce the following notations:

0) $O(n,t)$ denotes a set of t mutually orthogonal latin squares of order n.

1) $MOM(n,t)$ denotes a set of t mutually orthogonal $n \times n$ matrices.

2) $OA(n,t)$ denotes a set of orthogonal arrays of size n^2, depth t, n levels, and strength 2.

3) $Net(n,t)$ denotes a net of order n and degree t.

4) $Code(n,r,t;m)$ denotes a set of n code words each of length r such that any two code words are at least at Hamming distance $\geq t$ on an m-set Σ with m distinct elements. We remind the reader that such a code is also called $(t-1)$-error detecting code or $(t-1)/2$-error correcting code because such a code is capable of detecting up to $t-1$ errors and correct up to $(t-1)/2$ errors in each transmitted code word.

5) $PBIB(b,v,r,k,\lambda_1,\lambda_2)$ denotes a partially balanced incomplete block design with b blocks each of size k, v treatments with r replication of each, and association indices λ_1 and λ_2.

6) SR-Graph (A) denotes the strongly regular graph with incidence matrix A .

7) Non #(n,t) denotes an arrangement of n mutually non attacking rooks on the t-dimensional $n \times n$ chess board.

8) PG(2,s) denotes a finite projective plane of order s (not necessarily Desarguesian).

9) $\mathcal{E}(2,s)$ denotes a finite Euclidean plane of order s .

10) BIB(b,v,r,k,λ) denotes a balanced incomplete block design with b blocks each of size k, v treatments with r replications of each, and association index λ .

11) K-Graph (A) denotes the complete graph with incidence matrix A .

12) DIF(v,k,λ) denotes a difference set with parameters v, k, and λ .

13) BLRL(s) denotes a balanced set of ℓ-restrictional lattice design for s treatments. Note that a 1-restrictional balanced lattice design is simply a BIB design.

14) HAD(n) denotes a symmetric normalized Hadamard matrix of order n .

Hereafter we also adopt the following two notations:

i) A $\Longleftrightarrow$ B means A implies B and B implies A .

ii) A $\Longrightarrow$ B means A implies B . Whether or not B implies A is unstated.

XV. 3. The Result

Theorem

(a) For any pair of positive integers n and t we have:

1) $O(n,t) \iff MOM(n,t+2)$

2) $O(n,t) \iff OA(n,t+2)$

3) $O(n,t) \iff Net(n,t+2)$

4) $O(n,t) \iff Code(n^2, t+2, t+1; n)$

5) $O(n,t) \iff PBIB(n^2, n(t+2), n, t+2, O, 1)$

6) $O(n,t) \iff$ SR-Graph (A) where A is the incidence matrix associated with PBIB in 5).

7) $O(n,t) \iff Non\ \#(n^2, n^{t+2})$.

(b) If $t = n-1$ then also:

8) $O(n,n-1) \iff PG(2,n)$

9) $O(n,n-1) \iff \mathcal{E}(2,n)$

10) $O(n,n-1) \iff BIB(n^2+n+1, n^2+n+1, n+1, n+1, 1)$

11) $O(n,n-1) \iff Code(n^2+n+1, n^2+n+1, 2n; 2)$

12) $O(n,n-1) \iff$ K-Graph (A) where A is the incidence matrix associated with BIB in 10)

13) $O(n,n-1) \iff DIF(n^2+n+1, n+1, 1)$.

(c) If $n = p^m$ where p is a prime and m is a positive integer then also the following:

14) $O(p^m, p^m-1) \iff BLRL(p^m)$.

(d) If $n = 2r$ and $t = r-2$, $r \geq 3$ then the following are also true:

15) $O(2r,r-2) \Longrightarrow HAD(4r^2)$

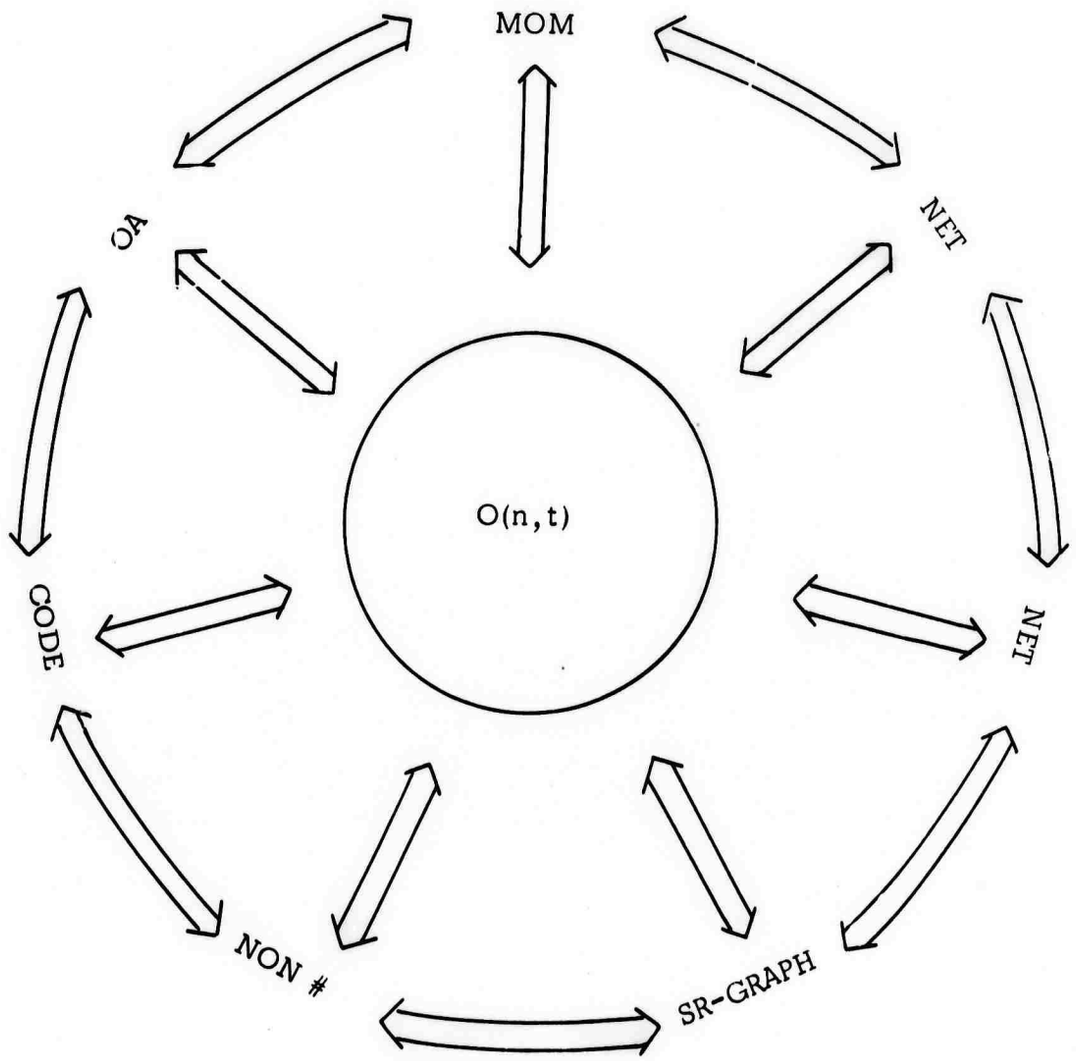
16) $O(2r,r-2) \Longrightarrow BIB(4r^2-1, 4r^2-1, 2r^2-1, 2r^2-1, r^2-1)$

17) $O(2r,r-2) \Longrightarrow Code(4r^2-1, 4r^2-1, 2r^2;2)$

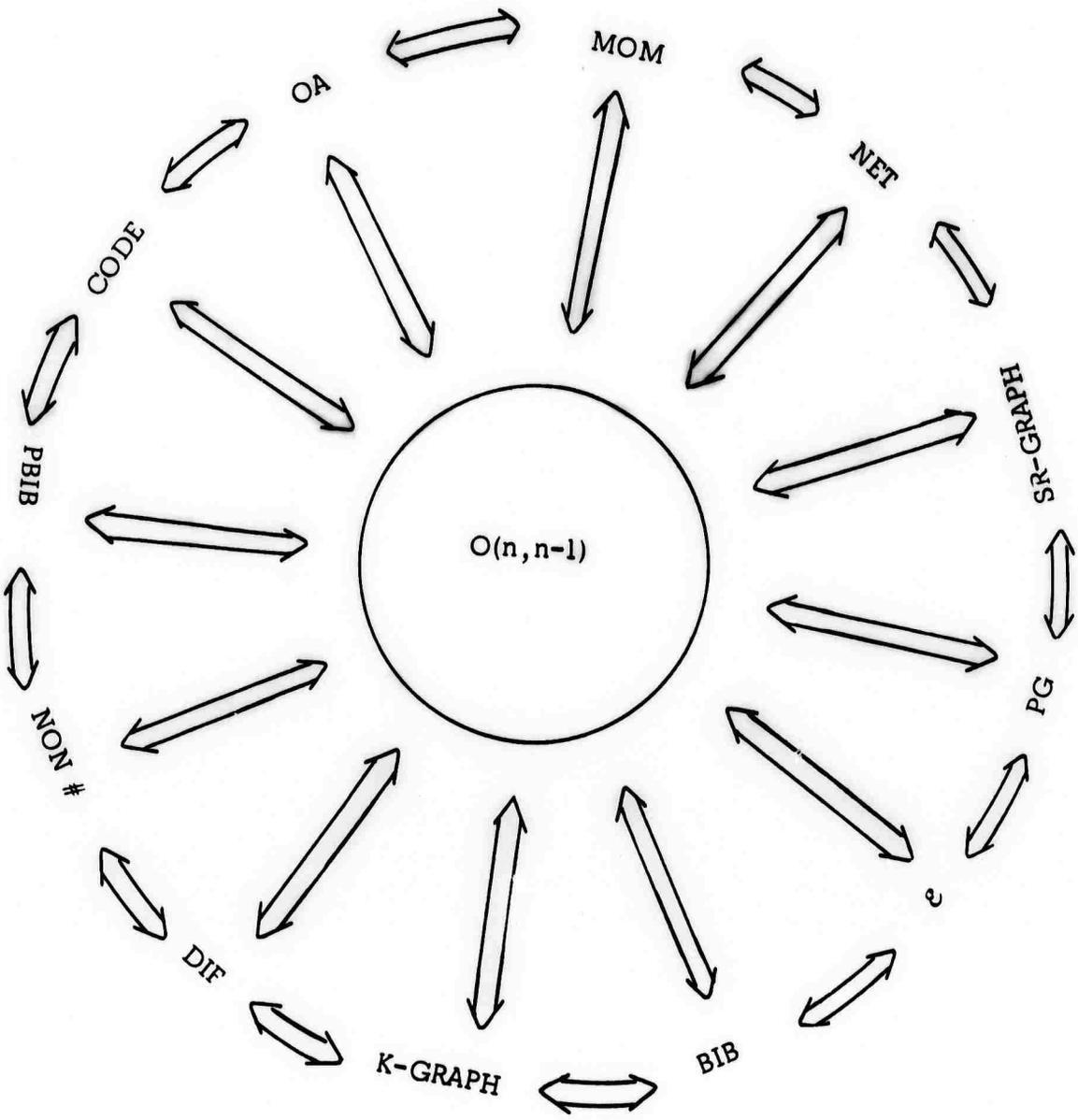
18) $O(2r,r-2) \Longrightarrow Code(8r^2, 4r^2, 2r^2;2)$

19) $O(2r,r-2) \Longrightarrow DIF(4r^2-1, 2r^2-1, r^2-1)$.

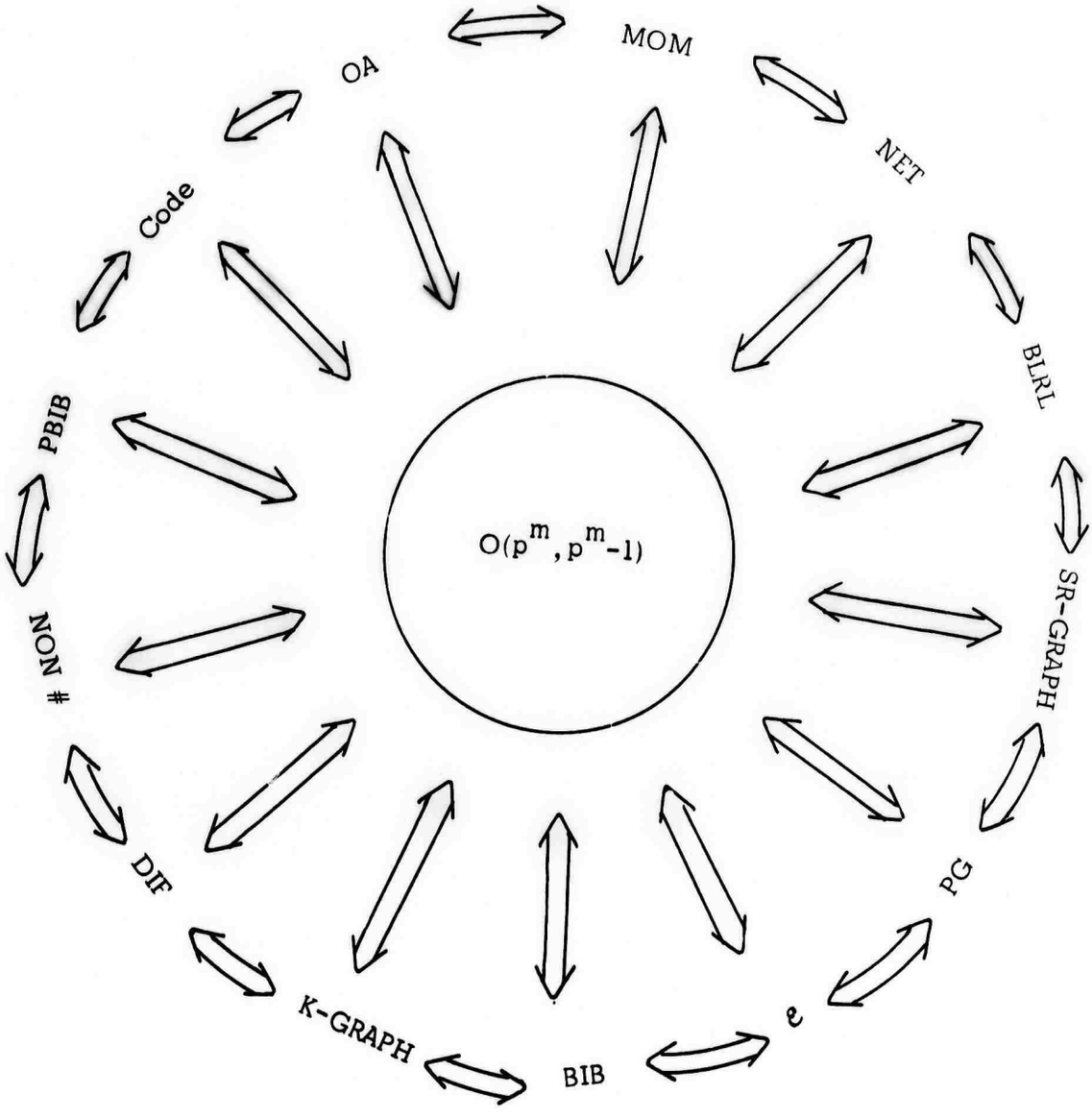
A complete schematic representation of this theorem can be demonstrated in four wheels which will be called "fundamental wheels of combinatorial mathematics". For the sake of compactness we shall omit the associated parameters with each system in these wheels except for $O(n,t)$. By knowing the values of n and t in the given $O(n,t)$ sets, then the reader can easily find the associated parameters with other systems in the wheels from the proper part of the above theorem.



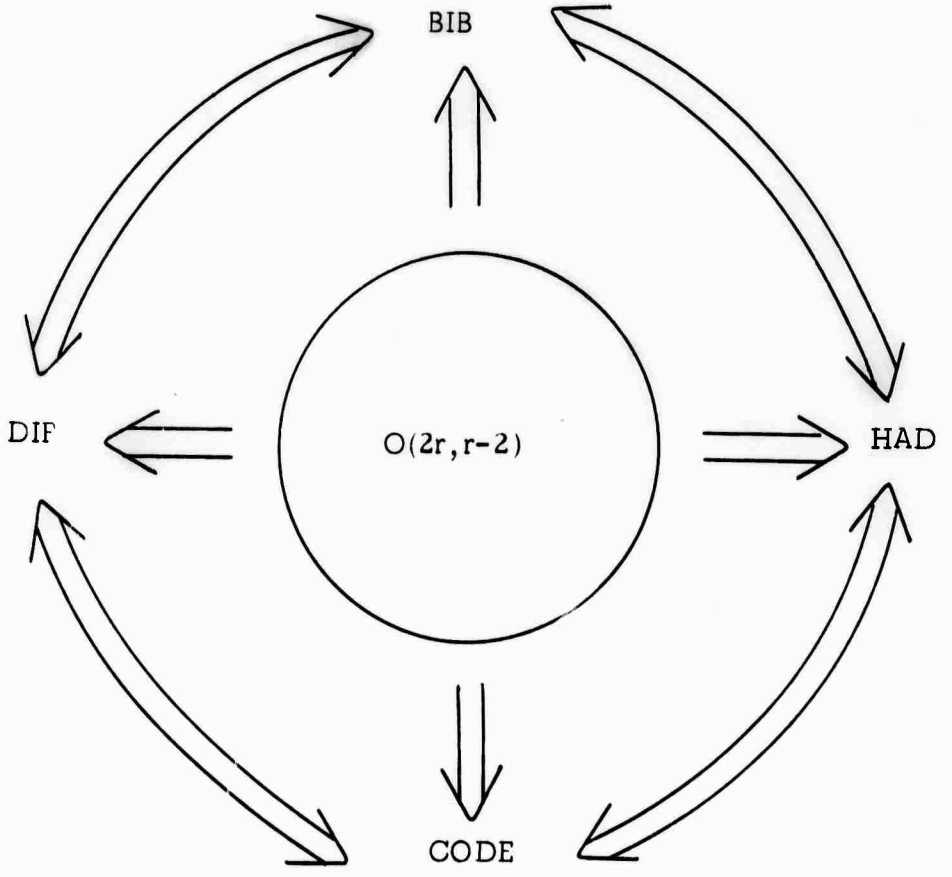
Wheel 1. For any positive integer n and t .



Wheel 2. For any positive integer n.



Wheel 3. For any prime p and positive integer m .



Wheel 4. For any positive integer $r \geq 3$.

(see also wheel 1)

XVI. Acknowledgements

This work was partially supported under the following research grants or contracts:

(i) Public Health Research Grant GM-05900, Cornell University

(ii) United States Army Contract Number DA-31-124-ARO-D-462, University of Wisconsin

(iii) National Science Foundation Grant GP-12881, Michigan State University

(iv) Office of Naval Research Contract N0014-A67-0305-0008, University of Illinois.

XVII. Literature Cited

1. Beckenbach, E. F. (ed.) [1964], Applied Combinatorial Mathematics, John Wiley and Sons, Inc., New York, London, Sydney.
2. Bose, R. C. [1938], On the application of the properties of Galois Fields to the problem of construction of Hyper-Graeco-Latin squares, Sankhyā 3: 323-338.
3. Bose, R. C. [1939], On the construction of balanced incomplete block designs, Annals of Eugenics 9: 343-399.
4. Bose, R. C. [1950], A note on orthogonal arrays (abstract), Annals of Mathematical Statistics 21: 304-305.
5. Bose, R. C. [1963], Strongly regular graphs, partial geometrics and partially balanced designs, Pacific Journal of Mathematics 13: 389-419.
6. Bose, R. C. Chakravarti, I. M., and Knuth, D. E. [1960], On methods of constructing sets of mutually orthogonal Latin squares using a computer, I. Technometrics 2: 507-516.
7. Bose, R. C. and Clatworthy, W. H. [1955], Some classes of partially balanced designs, Annals of Mathematical Statistics 26: 212-232.
8. Bose, R. C. and Shrikhande, S. S. [1959], On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order 4t + 2, Proceedings of the National Academy of Sciences, U.S.A. 45: 734-737.

9. Bose, R. C. and Shrikhande, S. S. [1960], On the construction of pairwise orthogonal Latin squares and the falsity of a conjecture of Euler, Transactions of the American Mathematical Society 95: 191-209.

10. Bose, R. C., Shrikhande, S. S. and Parker, E. T. [1960], Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, Canadian Journal of Mathematics 12: 189-203.

11. Bruck, R. H. [1951], Finite nets, I. Numerical invariants, Canadian Journal of Mathematics 3: 94-107.

12. Bruck, R. H. [1963], Finite nets, II. Uniqueness and embedding, Pacific Journal of Mathematics 13. 421-457.

13. Bruck, R. H. [1963], What is a loop? in "Studies in Modern Algebra" (editor, A. A. Albert), Math. Assoc. Amer. and Prentice Hall, Englewood Cliffs, New Jersey, pp. 59-99.

14. Dembowski, P. [1968], Finite Geometrics, Springer-Verlag, Berlin, Heidelberg, New York.

15. Euler, L. [1782], Recherches sur une nouvelle espèce des quarrés magiques, Verh. Zeeuwach Genoot. Wetenschappen, Vlissigen 9: 85-239.

16. Federer, W. T. [1955], Experimental Design, The Macmillan Company, New York.

17. Fisher, R. A. and Yates, F. [1957], Statistical Tables for Biological, Agricultural and Medical Research, 5th edition (first edition in 1938), Oliver and Boyd, Edinburgh and London.

18. Golomb, S. W. and Posner, E. C. [1964], Rook domains, Latin squares, affine planes, and error-distributing codes, IEEE Transactions on Information Theory IT-10: 196-208.

19. Hall, M. [1943], Projective planes, Transactions of the American Mathematical Society 54: 229-277.

20. Hall, M. Jr. [1967], Combinatorial Theory, Blaisdell Publishing Co., Waltham, Massachusetts, Toronto and London.

21. Hall, M. and Paige, L. J. [1955], Complete mappings of finite groups, Pacific Journal of Mathematics 5: 541-549.

22. Hedayat, A. [1968], On Singer 1-permutation, Unpublished paper, Biometrics Unit, Cornell University, Ithaca, New York.

23. Hedayat, A. [1969], On the theory of the existence, non-existence, and the construction of mutually orthogonal F-squares and latin squares, Ph. D. Thesis, Cornell University, Ithaca, New York.

24. Hedayat, A. [1969a], On the equivalence of a set of mutually orthogonal latin squares with other combinatorial systems, Paper RM-237, Dept. of Statistics and Probability, Michigan State University, East Lansing, Michigan.

25. Heydayat, A. [1970], An algebraic property of the totally symmetric loops associated with Kirkman-Steiner triple systems, Unpublished paper, Cornell University.

26. Hedayat, A. and Federer, W. T. [1969], An application of group theory to the existence and nonexistence of orthogonal latin squares, Biometrika 56: 547-551.

27. Hedayat, A. and Federer, W. T. [1970], On the equivalence of Mann's group automorphism method of constructing an O(n,n-1) set and Raktoe's collineation method of constructing a balanced set of ℓ-restrictional prime-powered lattice designs, Annals of Mathematical Statistics 41:1530-1540.

28. Hedayat, A. and Raktoe, B. L. [1970], A note on resolvable balanced incomplete block designs with parameters $v = 6t + 3$, $b = (2t+1)(3t+1)$, $r = 3t + 1$, $k = 3$, and $\lambda = 1$, Unpublished paper, Cornell University and University of Guelph.

29. Hedayat, A. and Seiden, E. [1969], On a method of sum composition of orthogonal latin squares. Paper No. RM-238, Dept. of Statistics and Probability, Michigan State University, East Lansing, Michigan.

30. Hedayat, A. and Seiden, E. [1969], Some contributions to the theory of F-squares, (To appear in the Annals of Mathematical Statistics).

31. Johnson, D. M., Dulmadge, A. L., and Mendelsohn, N. S. [1961], Orthomorphisms of groups and orthogonal Latin Squares I., Canadian Journal of Mathematics 13: 356-372.

32. Kempthorne, O. [1952], The Design and Analysis of Experiments, John Wiley and Sons, Inc., New York.

33. Levi, F. W. [1942], Finite Geometrical Systems, University of Calcutta, Calcutta, India.

34. MacNeish, H. F. [1922], Euler's squares, Annals of Mathematics 23: 221-227.

35. Mann, H. B. [1942], The construction of orthogonal Latin squares, Annals of Mathematical Statistics 13: 418-423.

36. Mann, H. B. [1943], On the construction of sets of orthogonal Latin squares, The Annals of Mathematical Statistics 14: 401-414.

37. Mann, H. B. [1944], On orthogonal Latin squares, Bulletin of the American Mathematical Society 50: 249-257.

38. Mann, H. B. [1949], Analysis and Design of Experiements, Dover Publications, Inc., N.Y.

39. Mann, H. B. (ed.) [1968], Error Correcting Codes, John Wiley and Sons, Inc., New York, London, Sydney, Toronto, pp. xii + 231.

40. Mullin, R. C. and Nemeth, E. [1969], A counter example to a direct product construction of Room squares, J. of Combinatorial Theory 7: 264-265.

41. Paige, L. J. [1951], Complete mappings of finite groups, Pacific Journal of Mathematics 1: 111-116.

42. Paige, L. J. and Tompkins, C. B. [1969], The size of the 10×10 orthogonal latin square problem, Proceedings of the Tenth Symposium in Applied Mathematics of the American Mathematics Society 10: 71-83.

43. Parker, E. T. [1959], Construction of some sets of mutually orthogonal latin squares, Proceedings of the American Mathematics Society 10: 946-949.

44. Parker, E. T. [1962], On orthogonal latin squares, Proceedings of Symposia in Pure Mathematics, American Mathematics Society 6: 43-46.

45. Peterson, W. W. [1961], Error-Correcting Codes, John Wiley and Sons, Inc., New York.

46. Raktoe, B. L. [1967], Application of cyclic collineations to the construction of balanced t-restrictional prime powered lattice designs, Annals of Mathematical Statistics 38: 1127-1141.

47. Raktoe, B. L. [1969], Combining elements from finite fields in mixed factorials, The Annals of Mathematical Statistics 40: 498-504.

48. Raktoe, B. L. and Federer, W. T. [1969], On irregular fractions of an s^m factorial, Unpublished paper, Biometrics Unit, Cornell University, Ithaca, New York.

49. Ryser, H. J. [1963], Combinatorial Mathematics, The Carus Mathematical Monographs No. 14, Mathematical Association of America and John Wiley and Sons, Inc., New York.

50. Sade, A. [1958], Groupïdes orthogonaux, Publicationes Mathematicae, 5: 229-240.

51. Silverman, R. [1960], A metrization for power sets with applications to combinatorial analysis, Canadian Journal of Mathematics 12: 158-176.

52. Singer, J. [1960], A class of groups associated with Latin squares, The American Mathematical Monthly 67: 235-240.

53. Stanton, R. G. and Horton, J. D. [1969], Composition of Room squares. Unpublished paper, York University.

54. Stevens, W. L. [1939], The completely orthogonalized Latin squares, Annals of Eugenics 9: 83-93.

55. Tarry, G. [1899], Sur le probleme d'Euler des n^2 officiers, L'Intermédiaire des Mathématiciens 6: 251-252.

56. Yates, F. [1937], The design and analysis of factorial experiements, Imperial Bureau of Soil Science, Technical Communication 35: 1-95.